Informationssicherheitsleitlinie für Dienstleister

1 Informationssicherheit im UKE-Konzern

Informationssicherheit stellt für das UKE ein äußerst wichtiges Qualitätsmerkmal der Datenverarbeitung dar, da alle wesentlichen strategischen und operativen Geschäftsprozesse im Klinikum durch Informationstechnologie (IT) maßgeblich unterstützt werden.

Mit der vorliegenden Informationssicherheitsleitlinie für Dienstleister werden die Informationssicherheitsorganisation und die dazugehörigen Prozesse dargestellt, die vom UKE zur Wahrung einer adäquaten Informationssicherheit bei beauftragten Dienstleistern eingefordert werden. Darüber hinaus werden Vorgaben für den beauftragten Dienstleister formuliert, die bei der Nutzung der IT-Systeme bzw. Daten des UKE zu berücksichtigen sind. Abschließend werden Anforderungen an die Administration und den Betrieb der IT-Systeme beschrieben.

2 Geltungsbereich

Die Informationssicherheitsleitlinie für Dienstleister gilt für alle Mitarbeiter des Dienstleisters, welche Daten für das UKE verarbeiten bzw. Zugang zu den Systemen des UKE haben. Vorsätzliche oder grob fahrlässige Verstöße gegen die Inhalte der Leitlinie können zu vertragsrechtlichen Konsequenzen führen.

Die Informationssicherheitsleitlinie für Dienstleister dient auch zur Sensibilisierung aller Nutzer von Informationen/IT-Ressourcen. Sie sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken, verantwortungsbewusst mit den Informationssystemen und den zu verarbeiteten Daten/Informationen umgehen und bei Unregelmäßigkeiten unverzüglich das UKE informieren.

Die Informationssicherheitsleitlinie für Dienstleister wird fortlaufend weiterentwickelt. Für die redaktionelle und inhaltliche Pflege und Weiterentwicklung der Leitlinie ist der Informationssicherheitsbeauftragte des UKE zuständig; bei Änderungen werden die betroffenen Dienstleister von den Auftraggebern informiert.

3 Sicherheitsziele des UKE-Konzern

4 Informationssicherheitsschulung

Die Mitarbeiter des Dienstleisters sollten regelmäßig durch entsprechende Security Awareness Maßnahmen geschult werden, um sich der Bedeutung der Informationssicherheit für das Unternehmen bewusst zu sein. Der Inhalt der Schulungen sollte mindestens die zentralen Regelungen der Informationssicherheitsleitlinie für Dienstleister sowie eine Einführung in die Bedeutung der Informationssicherheit für das UKE umfassen. Zusätzlich sollten die jeweils relevanten Problematiken wie z.B. Email, SPAM, Viren oder Social Engineering angesprochen werden.

5 Verpflichtung der Mitarbeiter auf das Datengeheimnis

Sämtliche Mitarbeiter des Dienstleisters, die technisch an der Erbringung von Diensten wie E-Mail und/oder Internet mitwirken, also insbesondere Administratoren im Bereich E-Mail/Internet, Netzwerktechniker und Beschäftigte mit ähnlichen Tätigkeitsgebieten, die Zugriff auf E-Mails und/oder IT-Kommunikation haben können, sind darüber zu informieren, dass es ihnen untersagt ist, sich oder andere über das für die Erbringung der Telekommunikationsdienste oder für den Betrieb der Telekommunikationsnetze oder -anlagen einschließlich des Schutzes der technischen Systeme erforderliche Maß hinaus, Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation zu verschaffen und sie Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den vorstehend genannten Zweck verwenden dürfen. Die Verpflichtung auf das Fernmeldegeheimnis besteht auch nach Beendigung der Tätigkeit fort.

6 Umgang mit Informationen des UKE

Alle Informationen (Daten/Dokumente/etc.) des UKE müssen folgendermaßen behandelt werden:

Zugriff	Bearbeiter- und Leserkreis ist fest definiert. Dies sind die Mitarbeiter, die diese Daten zur Erfüllung übertragener Aufgaben benötigen.
Übertragungswege	Elektronisch: Ein unverschlüsselter Transport ist nur innerhalb des abgesicherten Firmen-Netzwerks zugelassen, bei allen anderen Wegen müssen die Daten verschlüsselt sein (z.B. mobile Datenträger, elektronischer Versand). Andere: Eine nicht-elektronische Weitergabe außerhalb des Unternehmens erfolgt ausschließlich in verschlossenen Umschlägen/Behältern. Eine Übertragung per Fax ist nicht zulässig.
Ablage	Elektronische Ablage: Eine Speicherung auf mobilen Endgeräten ist nur mit geeigneter Verschlüsselung zulässig Andere: Die Ablage ist nur innerhalb der hierfür vorgesehenen Büroräume zugelassen. Eine Vervielfältigung sollte mit Bedacht erfolgen. Die Dokumente dürfen nicht offen bzw. unbewacht in Postfächern oder auf Schreibtischen liegen.
Druck	Der Ausdruck auf Druckern, die nicht unmittelbar am Arbeitsplatz aufgestellt sind, ist erlaubt. Die Ausdrucke sind unverzüglich abzuholen.
Vernichtung	Papiere sind mittels entsprechendem Aktenvernichter (min. Sicherheitsstufe P-4 DIN 66399) zu vernichten. Defekte und ersetzte Datenträger dürfen nur außer Haus gelangen, wenn hierzu geeignete Sicherheits-Vereinbarungen (z.B. verplombte Datenträgertonnen anschließende Vernichtung nach min. Sicherheitsstufe O-4 DIN 66399) mit Dienstleistern existieren oder die Datenträger physisch (nach min. Sicherheitsstufe O-4 DIN 66399) zerstört wurden. Bei der Vernichtung sind auch Kopien mit zu berücksichtigen.

Bei Entnahme von wieder beschreibbaren Datenträgern aus dem Betrieb, z.B. zur anderweitigen Nutzung oder Veräußerung, muss eine Löschung so erfolgen, dass eine Wiederherstellung der Daten unmöglich ist.

7 Vorgaben für die IT-Anwender

Die Mitarbeiter müssen sich ihrer Verantwortung beim Umgang mit den auf den IT-Systemen gespeicherten Daten bewusst sein. Hierzu sind die Mitarbeiter in sicherheitsrelevante Aspekte, die ihr Aufgabengebiet betreffen, entsprechend einzuweisen. Dies kann sowohl durch externe Fortbildungen als auch durch interne Schulungen erfolgen.

Die Mitarbeiter haben sicherzustellen, dass sie nur Anwendern Zugriff auf Daten ermöglichen, die dazu berechtigt sind. Die Mitarbeiter sind verpflichtet, sicherheitsrelevante Ereignisse und unerklärliches Systemverhalten sofort dem Leiter GB-IT oder dem Informationssicherheitsbeauftragten mitzuteilen.

7.1 Umgang mit Passwörtern

Sollte die Authentisierung gegenüber dem Betriebssystem und den Anwendungen per Benutzerkennung und Passwort erfolgen, ist jedem Mitarbeiter eine individuelle Benutzerkennung zuzuweisen. Die von den Mitarbeitern benutzten Passwörter müssen geheim gehalten werden und dürfen nicht an andere Personen weitergegeben werden. Besonders dürfen Passwörter nicht öffentlich zugänglich notiert werden. Sofern der Verdacht besteht, dass Passwörter auch anderen Personen bekannt geworden sind, müssen diese geändert werden.

Insgesamt werden an die Passwörter folgende Mindestanforderungen gestellt:

- Die Mindestlänge beträgt 8 Zeichen, es müssen mindestens drei der vier Kriterien Großbuchstabe/Kleinbuchstabe/Zahl oder Sonderzeichen erfüllt sein.
- die Höchstgültigkeitsdauer beträgt 180 Tage; anschließend müssen neue Passwörter verwendet werden, die sich von den zehn vorherigen unterscheiden.
- Der Benutzer sollte nicht in der Lage sein, sein Passwort eigenständig innerhalb von einem Tag zweimal zurückzusetzen.
- Um die Gefahr zu reduzieren, dass Passwörter erraten werden, dürfen keine Trivial-Passwörter verwendet werden.

Sollte das Passwort bei der Anmeldung eines Nutzers dreimal falsch eingegeben werden, wird das Konto für dreißig Minuten gesperrt.

7.2 Vorgaben zum aufgeräumten Schreibtisch und leerem Bildschirm

Beim Verlassen des Arbeitsplatzes sind Unterlagen mit Daten des UKE so aufzubewahren, dass sie von nichtautorisierten Personen nicht ohne Aufwand zur Kenntnis genommen werden können. Gleiches gilt, wenn Besucher sich in den Räumen aufhalten. Unterlagen und Datenträger, die vertrauliche Daten des UKE enthalten, werden nicht über den normalen Hausmüll entsorgt, sondern gesondert vernichtet (Siehe Kapitel 6). Arbeitsplatz-Clients, mit denen Daten des UKE verarbeitet werden können, sind beim Verlassen des Raumes per Bildschirmschoner zu sperren; dies gilt insbesondere dann, wenn Unbefugte (z. B. Besucher, Mitarbeiter, die nicht am Geschäftsvorgang beteiligt sind) Zugang zum System haben könnten. Eine Deaktivierung erfolgt nur nach erfolgreicher Authentisierung per Passwort (Clear-Screen-Policy).

Des Weiteren sollte der Bildschirmschoner so konfiguriert werden, dass dieser nach maximal 15 Minuten Nichtbenutzung des Rechners automatisch aktiv wird.

7.3 Hardware-Nutzung

7.4 Zugriff auf das Unternehmensnetz

Der Zugriff auf das Unternehmensnetz des UKE durch beauftragte Dienstleister ist ausschließlich über eine abgesicherte Verbindung und mit Geräten, die die Anforderungen dieser Informationssicherheitsrichtlinie für Dienstleister erfüllen, gestattet. Des Weiteren muss das hierfür genutzte Gerät mit aktuellen Sicherheitsupdates ausgestattet sein.

7.5 Verhalten gegenüber Dritten

7.5.1 Betriebsfremde

Auskünfte über die Struktur der internen Systemumgebung, die eingesetzte Hard- & Software sowie die verwendeten Passwörter sind grundsätzlich und gegenüber jeder nicht autorisierten Person, auch vermeintlich autorisierten Personen, untersagt. Dies gilt für persönliche Gespräche ebenso wie für Telefonate oder E-Mails. Wenn die Identität eines Gesprächspartners nicht zweifelsfrei ermittelt werden kann, sind zusätzliche Prüfungen erforderlich, z.B. durch einen Rückruf bei einer bereits bekannten Telefonnummer. Die Kenntnis unternehmensinterner Details ist keine ausreichende Legitimation. Anrufe, die Anfragen zur Informationsauskunft oder Serviceanfragen enthalten, sollten im Zweifel vor Erfüllung in die Warteschleife gestellt und vom Angerufenen in Ruhe überdacht werden. Dies verhindert übereilte Aktionen. Im Zweifel ist die Informationsauskunft zu verweigern und die Anfrage zu eskalieren.

7.5.2 Unterauftragnehmer

Sollte der Dienstleister des UKE Unterauftragnehmer beauftragen, so muss dies vom UKE schriftlich genehmigt werden. Der Unterauftragnehmer verpflichtet sich vertraglich, die Sicherheitsvorgaben des UKE zu beachten; diese beinhalten insbesondere die vorliegende Informationssicherheitsleitlinie für Dienstleister.

Unterauftragnehmer umfassen sowohl Dienstleister als auch Lieferanten, wenn diese oder ihre IT-Systeme direkt oder indirekt für das UKE eingesetzt werden.

Die Weitergabe eines Auftrages an Personen und Institutionen außerhalb des benannten Mitarbeiterkreises ist dem Dienstleister nur nach vorheriger Genehmigung durch das UKE gestattet. Auch im Fall einer genehmigten Weitergabe überträgt sich die Genehmigung für den Remote-Zugriff nicht automatisch auf Dritte, sondern bezieht sich weiterhin nur auf die vertraglich benannten Mitarbeiter des Dienstleisters.

Die Einhaltung der weitergegebenen Richtlinien und Anforderungen liegt im Verantwortungsbereich des Dienstleisters und wird durch eine eigene Dienstleistersteuerung inklusive der Durchführung von Kontrollen bei den eingesetzten Dienstleistern und Lieferanten belegt.

8 Vorgaben für IT-Administratoren

Die IT-Administratoren besitzen im Hinblick auf die Informationssicherheit eine besondere Verantwortung. Grundsätzlich gilt, dass die IT-Administratoren Sicherheitseinstellungen an den Komponenten vornehmen können und müssen, um beispielsweise Systeme neu aufzusetzen und Software zu installieren. Gleiches gilt für die Einrichtung, Änderung und Überwachung von Kommunikationsverbindungen.

Im Folgenden werden daher Grundsätze beschrieben, nach denen die IT-Administration für das UKE und bei vom UKE eingesetzten Dienstleistern erfolgen soll. Diese gelten ergänzend zu den Vorgaben für IT-Anwender.

8.1 Serveradministration

Die Administration von Betriebssystemen, Datenbanken und Anwendungen erfordern einen privilegierten Zugriff auf die jeweiligen Systeme. Privilegierte Zugriffe sind daher nur unter größter Sorgfalt zu verwenden.

Die Administration der Server erfolgt mit individuellen Benutzerkennungen, diese Administratorkonten dürfen nur für administrative Tätigkeiten verwendet werden. Root-Kennungen sind möglichst nur im Ausnahmefall zu verwenden. Passwörter befinden sich beispielsweise in einem verschlossenen und signierten Umschlag in einem Tresor. Die Nutzung des Passworts erfolgt nach dem 4-Augen-Prinzip und wird protokolliert.

Wenn Leistungen von Dritten erbracht werden, sind diese zu dokumentieren (z.B. Ticketsystem des Dienstleisters bzw. Unterauftragnehmer) und nach der Leistungserbringung ist eine Abnahme durch die IT-Abteilung durchzuführen.

Die Verantwortungen innerhalb der IT-Abteilung sind festgelegt. Für jedes System und jede Anwendung wurden Ansprechpartner und Stellvertreter benannt, die für die Administration verantwortlich sind.

An normale Benutzer dürfen keine Administrationsrechte vergeben werden. Ggf. sind spezielle Benutzerkennungen für die Administration bestimmter Software einzurichten. Benutzer mit Administrationsrechten bzw. mit Nutzungsrechten für bestimme Systemkommandos müssen bei Bedarf aufgelistet werden können.

Im Rahmen der Serveradministration zur Kenntnis gelangte Daten dürfen nicht anderen Personen offenbart werden.

8.2 Change-Management

Von Herstellerseite aus Sicherheitsgründen empfohlene Software-Updates werden auf Arbeitsplatzsystemen und Servern zeitnah installiert, sofern hiermit keine Risiken anderer Art verbunden sind.

Änderungen an IT-Systemen erfolgen im Rahmen des Change-Managements und sollten außerhalb des Systems mit Datum und Uhrzeit der Änderung, der Grund der Änderung, der durchgeführten Tätigkeit sowie dem Namen des jeweiligen Administrators dokumentiert werden.

Besonders sicherheitskritische Änderungen, mit Auswirkungen auf das UKE, sind in Absprache mit dem Leiter GB-IT des UKE bzw. dem Informationssicherheitsbeauftragten des UKE durchzuführen, und wenn möglich vorab auf einem Testsystem zu überprüfen. Erst nach abschließender Bewertung der Testergebnisse sind Änderungen an den Produktivsystemen vorzunehmen.

Besonders sicherheitsrelevante Tätigkeiten sind u.a.

- Release- und Versionswechsel
- Neuanlegen von privilegierten Benutzerkennungen
- Neuinstallation von sicherheitskritischen Programmen
- Änderung von sicherheitskritischen Parametern
- Grundlegende Systemänderungen

Regelmäßige operative Tätigkeiten sind in der Regel nicht besonders sicherheitskritisch und bedürfen nicht der Freigabe durch das UKE.

8.3 Sichere Entwicklung

Um Vertrauen in die korrekte Funktion eines Systems für das UKE zu haben, muss sichergestellt werden, dass seine Komponenten während ihres gesamten Lebenszyklus nicht unbefugt manipuliert wurden. Dies gilt auch für die Entwicklungsumgebung, in der sichergestellt werden muss, dass auch an den Quellen und Entwicklungsdoku-

menten zu keiner Zeit unbefugte Änderungen vorgenommen wurden. Die Sicherheit der Entwicklung betrifft daher die Maßnahmen, die von den Entwicklern getroffen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit der Entwicklungsumgebung während des gesamten Lebenszyklus sicherzustellen.

8.3.1 Schutz von Test-Daten

Entwicklungs- und Testumgebungen sowie produktive IT-Systeme, sind voneinander zu trennen. Für Tests sind, sofern möglich, Testdaten zu erzeugen (z. B. mittels eines Testdatengenerators). Der Test von Software ist nur in der dafür vorgesehenen Testumgebung zulässig. Dabei ist sicherzustellen, dass der produktive Betrieb nicht in Mitleidenschaft gezogen wird. Personenbezogene, vertrauliche oder geheime Daten des UKE sind vor der Übernahme von produktiven IT-Systemen in die Testsysteme so zu verfälschen, dass ein Rückschluss auf die Original-Daten nicht mehr möglich ist. Die verfälschten Daten unterliegen den gleichen Informationssicherheitsanforderungen wie die Original-Daten. Benutzte Informationen sind nach Durchführung der Tests zu löschen. Zugriffsberechtigungen, die für laufende IT-Systeme gelten, müssen auch für Testanwendungen beachtet werden.

8.3.2 Schutz des Quellcodes

Der Programmquellcode mit Relevanz zum UKE ist vor unbefugten Zugriff zu schützen. Änderungen sollten gemäß dem Change-Management nachvollziehbar sein.

8.3.3 Sicherheit bei Entwicklungs- und Unterstützungsprozessen

Alle Abläufe und Vorgänge, die IT-Systeme berühren, sind so zu gestalten, dass das jeweils angestrebte Informationssicherheitsniveau ganzheitlich erreicht und beibehalten wird. Es muss sichergestellt sein, dass Sicherheit und Überwachungsverfahren der IT-Systeme nicht durch Änderungen kompromittiert werden. Wenn Änderungen an gekauften Softwarepaketen durchgeführt werden, sind die Auswirkungen auf bestehende Regelungen und Sicherheitsmaßnahmen zu klären. Änderungen dürfen nur erfolgen, wenn dies lizenzrechtlich und aufgrund der Wartungsverträge zulässig ist.

8.4 Benutzerverwaltung

Bei der Vergabe von Zugriffsrechten auf Daten und IT-Systeme des UKE ist das Prinzip der minimalen Rechtevergabe zu berücksichtigen, d.h. Zugriffsberechtigungen werden nur in dem Maße erteilt, wie sie zur Aufgabenerfüllung minimal erforderlich sind. Es werden Rollen definiert, denen Zugriffsberechtigungen zugeordnet werden. Für Systeme, Anwendungen und Daten werden Eigentümer und Stellvertreter benannt, die für die Definition von Rollen und zugeordneten Berechtigungen verantwortlich sind. Zugänge zu Systemen sind ausschließlich über eindeutige Kennungen gestattet, über die die entsprechenden Nutzer identifiziert werden können. Die Nutzerkennung sollte dabei keinen Hinweis auf die damit verbundenen Berechtigungen zulassen (z.B. Administratorkonto).

8.4.1 Management von privilegierten Berechtigungen

Privilegiertere Zugangs- und Zugriffsberechtigungen, z.B. in Verbindung mit Administrator-Konten, müssen für alle Systeme und Netzwerke identifiziert und kontrolliert werden. Administrative Zugänge sollten nicht als standardmäßige Benutzerkonten verwendet werden, sondern nur dann zum Einsatz kommen, wenn die entsprechenden Rechte auch benötigt werden. Weiterhin sind administrative Zugänge ausschließlich personenspezifisch zu vergeben. Generische Admin-Accounts sind zu vermeiden, da somit keine eindeutige Identifikation des entsprechenden Nutzers sichergestellt ist.

Die Nutzung von privilegierten bzw. administrativen Zugängen für automatisierte Funktionen oder Batch-Skripte ist nach Möglichkeit zu vermeiden. Ansonsten sollten die genutzten Passwörter geschützt und regelmäßig geändert werden.

8.4.2 Passwörter für Dienstkonten

Die verwendeten Passwörter für Dienstkonten sollen den folgenden Regelungen entsprechen:

- Länge: Mindestens 14 Zeichen
- Komplexität: Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Mindestalter: 1 Tag
- maximales Alter: Abhängig vom Schutzbedarf des Systems und Aufwand der Änderung
- Historie: 24 Passwörter

8.4.3 Kontrolle von Berechtigungen

Gemäß den zugeteilten Verantwortlichkeiten und Zuständigkeiten ist eine halbjährliche Überprüfung der vergebenen Zugangs- und Zugriffsberechtigungen vorzunehmen. Dabei sind folgende Themengebiete zu prüfen:

- Kontrolle von nicht mehr benötigten Zugängen (z. B. Ex-Mitarbeiter)
- Berechtigungen von privilegierten Nutzern oder Administratoren
- Abgleich von Soll- und Ist-Berechtigungen gemäß dem „Need-To-Know“-Prinzip
- Korrektheit von Rollen- bzw. Gruppenzuordnungen
- Möglichkeit der adäquaten Identifizierung von Nutzern über Benutzernamen
- Berechtigungen von externen Nutzern/Dienstleistern

8.5 Protokollierung

Auf den relevanten Systemen für das UKE ist eine Protokollierung einzurichten. Erfasst werden sollten alle sicherheitsrelevanten Ereignisse, welche regelmäßig ausgewertet werden.

8.6 Datensicherung

Um die Verfügbarkeit der Unternehmensdaten und –systeme sicherzustellen, werden folgende Vorgaben umgesetzt:

- Alle Daten des UKE oder für die Erbringung der vom UKE beauftragten Dienstleistung müssen entsprechend ihrer definierten Notwendigkeit regelmäßig gesichert werden.
- Die notwendigen Sicherungszeiträume und Wiederherstellungsfristen sollten in einem Datensicherungskonzept definiert werden und kann auf Verlangen des UKE eingesehen werden.
- Die Datensicherungsträger müssen jederzeit eindeutig identifiziert werden können.
- Alle Medien auf denen Daten des UKE gesichert werden, sind mit einem geeigneten Verfahren zur Verschlüsselung gegen unberechtigten Zugriff und Einblick in Daten und Informationen zu sichern. Es ist darauf zu achten, dass ein ausreichend starker Schlüssel verwendet wird.

9 Zutrittskontrolle

Die Räumlichkeiten des Dienstleisters sind vor unbefugten Zutritt entsprechend dem Schutzbedarf der zu verarbeitenden Informationen des UKE zu sichern. Die Ausgabe und Rücknahme sowie die Berechtigungen der Schlüssel/Codekarte/Token sollten dokumentiert und regelmäßig (min. einmal jährlich) überprüft werden.

10 Umgang mit Sicherheitsvorfällen

Das Auftreten von Sicherheitsvorfällen kann nicht immer vermieden werden, wobei die damit verbundenen Probleme oft auch erst durch eine falsche Reaktion der beteiligten Personen entstehen können. Beispielweise können Daten gelöscht werden, welche notwendig gewesen wären, um den Vorfall genauer zu untersuchen. Daher muss

das richtige Verhalten beim Auftreten eines Sicherheitsvorfalls sowie dessen Behandlung dokumentiert sein. Es muss sichergestellt werden das die Reaktions-, Entscheidungs- und Handlungsfähigkeit sichergestellt ist, um zum einen die wirksame Einhaltung eines angemessenen Informationssicherheitsniveaus zu gewährleisten und zum anderen eventuelle Schäden zu minimieren. Ein Sicherheitsvorfall mit möglicher Relevanz für Daten oder Systeme des UKE, bzw. deren Patienten, Beschäftigte und/oder Studierende ist ohne jeden Verzug dem UKE anzuzeigen. Hierzu sind das Postfach informationssicherheit@uke.de oder die +4915222837981 zu nutzen.

11 Notfallplanung

Vom Dienstleister sollte ein Notfallhandbuch zur Vermeidung und Behebung von Notfällen bereitgestellt werden. Im Rahmen dieses Handbuchs werden mögliche Notfälle identifiziert und die einzuleitenden Maßnahmen zur Vermeidung und Behebung dieser Notfälle geplant. Es werden entsprechend dieser Notfallplanung die benötigten Ressourcen bereitgestellt, um den Betrieb der IT entsprechend den Anforderungen wiederherstellen zu können. Grundsätzlich gilt, dass

- Alle wichtigen Systeme redundant ausgelegt sind.
- Es werden ausreichend Ersatzsysteme und -hardware bereitgehalten, um bei Ausfall einzelner Komponenten schnellstmöglich den Betrieb wieder aufnehmen zu können.
- Es wurden Serviceverträge mit den relevanten Dienstleistern bzw. Unterauftragnehmern geschlossen, um bei Ausfall von Systemen und System-Komponenten schnellstmöglich den Betrieb wieder aufnehmen zu können.

Version	Änderungen gegenüber der letzten Fassung:
01	Neuerstellung des Dokuments