THE LOGISTICS FLOW.

Data Security Standards

für Business Partner der TBDS

Version: 1.0
Gültig ab: 01. Mai 2018

Kontakt: TB Digital Services GmbH,
Oskar-Schlemmer-Straße 19-21,
80807 Munich
info@rio.cloud

THE LOGISTICS FLOW.

Inhalt

1. Zweck

Das Dokument dient der Information externer Partner der TBDS in Bezug auf die Anforderungen zur Informationssicherheit bei TBDS. Das Dokument beschreibt die grundlegenden Anforderungen der TBDS an einen sicheren und ordnungsgemäßen Betrieb. Weitere TBDS interne Regelungen sollen einem Partner der TBDS, welcher Dienstleistungen in Zusammenhang mit der Informationsverarbeitung erbringt nach Abschluss einer Vertraulichkeitserklärung zur Berücksichtigung zur Verfügung gestellt werden.

2. Informationssicherheit von TBDS IuK-Systemen

Informationen stellen vergleichbar zu Produktionsanlagen wichtige Vermögenswerte der TBDS dar.

Die Geschäfts- und Produktionsprozesse der TBDS laufen nur mit den korrekten Informationen zum richtigen Zeitpunkt am richtigen Ort ab. Ein wirksamer Schutz dieser Informationswerte in den TBDS Informations- und Kommunikations-Systemen (IuK-Systeme) ist für den Geschäftserfolg der TBDS von entscheidender Bedeutung.

Da die Informationswerte täglich einem breiten Spektrum von Bedrohungen wie:

- Zerstörung von Informationen durch Computerviren
- Diebstahl von Informationen durch Auspionieren von Passwörtern
- Diebstahl von Datenträgern oder Computern
- Ausfall von TBDS IuK-Systemen durch Energieausfälle, Sabotage oder Vandalismus
- Zerstörung wichtiger Daten durch Feuer oder Wasser

ausgesetzt sind, sind diese besonders zu schützen.

Ein wirksamer Schutz kann nur durch eine Vielzahl ineinandergreifender Maßnahmen erreicht werden.

Zu den erforderlichen Maßnahmen des Informationsschutzes gehören neben den bereits im TBDS Regelwerk zur Informationssicherheit aufgeführten Maßnahmen, insbesondere:

- das Sicherheitsbewusstsein aller Mitarbeiter eines IT-Service Providers,
- die Einhaltung der festgelegten Prozesse und Verfahren,
- der angemessene Umgang mit und Schutz von Informations- und Kommunikationsgeräten und Software sowie
- ein risikoorientiertes angemessenes Reporting des Designs und der Effektivität der Informationssicherheit des IT-Service Providers an TBDS,
- das Recht der regelmäßigen Überprüfung (auch beim IT-Service Provider).

Unter „risikoorientiert“ ist zu verstehen, dass das Risiko der Geschäftsprozesse der TBDS Berücksichtigung findet. Hierzu ist das Risiko gemeinsam mit der TBDS zu bestimmen.

2.1. Verantwortung für die Informationssicherheit der IuK-Systeme

Jeder IT-Service Provider mit Rechten zur Konfiguration von TBDS IuK- Systemen, ist für eine - den Informationssicherheitsrichtlinien der TBDS entsprechende - Konfiguration der IuK-Systeme in seinem Zuständigkeitsbereich verantwortlich. Insbesondere ist:

- jeder Anwendungsentwickler und Systemarchitekt eines TBDS Service Providers für einen den Informationssicherheitsrichtlinien der TBDS entsprechenden risikoorientierten Entwurf, die entsprechenden Spezifikationen, Test und Migration der IuK- Systeme der TBDS verantwortlich.
- jeder betriebsverantwortliche Mitarbeiter eines TBDS Service Providers für eine den Richtlinien der TBDS entsprechenden risikoorientierte Betriebssicherheit der IuK-Systeme in seinem Zuständigkeitsbereich verantwortlich. Hierzu gehört, dass der IT-Service Provider auf mögliche Bedrohungen achtet, diese den Ansprechpartnern der TBDS aufzeigt und eine unnötige Gefährdung von Informationen vermeidet.

2.2. Ansprechpartner für Informationssicherheit

Jeder IT-Service Provider muss für Fragen der Informationssicherheit einen Information Security Officer (ISO) benennen, insofern TBDS dies vertraglich als Anforderung definiert. Dieser ist Ansprechpartner für den CISO der TBDS und die ISOs der Volkswagen Truck & Bus Teilkonzerne und Unternehmen.

Für alle unternehmensübergreifenden bzw. konzernweiten Fragestellungen ist der Chief Information Security Officer (CISO) der TBDS der zuständige Ansprechpartner der IT Service Provider. Dies gilt insbesondere bei Fragen zu Informations-sicherheitsvorfällen und deren Handhabung.

Bei Fragen zum Schutz personenbezogener Daten sind Ansprechpartner in Deutschland die Datenschutzbeauftragten und im Ausland die Datenschutzkoordinatoren.

3. Verantwortung der IT-Service Provider der TBDS

Jeder IT-Service Provider, ist für eine - den Informationssicherheitsreglungen der TBDS entsprechende Konfiguration der TBDS IuK-Systeme in seinem Zuständigkeitsbereich verantwortlich. Insbesondere ist:

- jeder Anwendungsentwickler und Systemarchitekt eines TBDS Service Providers für einen den Informationssicherheitsrichtlinien der TBDS entsprechenden risikoorientierten Entwurf, die entsprechenden Spezifikationen, Test und Migration der IuK-Systeme der TBDS verantwortlich.
- jeder betriebsverantwortliche Mitarbeiter eines TBDS Service Providers für eine den Richtlinien der TBDS entsprechenden risikoorientierte Betriebssicherheit der IuK-Systeme in seinem Zuständigkeitsbereich verantwortlich. Hierzu gehört, dass der IT-Service Provider auf mögliche Bedrohungen achtet, diese den Ansprechpartnern der TBDS aufzeigt und eine unnötige Gefährdung von Informationen vermeidet.

Unter „risikoorientiert“ ist zu verstehen, dass das Risiko der Geschäftsprozesse der TBDS Berücksichtigung findet. Hierzu ist das Risiko gemeinsam mit der TBDS zu bestimmen.

Alle IT-Service Provider der TBDS sind verpflichtet Risiken für die TBDS, welche durch die Nutzung der vom IT-Service Provider zu Verfügung gestellten IT-Services / IuK-Systeme für die TBDS entstehen können, zu identifizieren und in enger Zusammenarbeit mit der IS Organisation der TBDS abzustimmen.

Je nach Anforderung der TBDS und der Aufgabe sind durch die IT-Service Provider:

- die durch die TBDS definierten Ziele der Informationssicherheit geeignet zu unterstützen,
- das TBDS Regelwerk der Informationssicherheit als verbindliches Rahmenwerk bei allen IT- Services des IT-Service Providers zu beachten,

- basierend auf den Informationssicherheitsanforderungen der TBDS ggf. ergänzende Anweisungen im Verantwortungsbereich des IT-Service Providers zu erlassen,
- ausreichende Ressourcen für die Einrichtung, Umsetzung, den Betrieb, die Überwachung, Überprüfung, Instandhaltung und die kontinuierliche Verbesserung des Managements der Informationssicherheit bereitzustellen,
- Kriterien für ein akzeptables Sicherheitsniveau der TBDS IT-Services gemeinsam mit der TBDS zu bestimmen,
- im Rahmen des Risikomanagements des IT-Service Providers die Verfügbarkeit, Vertraulichkeit und Integrität von Informationswerten / IT-Services / IuK-Systemen im Sinne der Anforderungen der TBDS zu berücksichtigen,
- für identifizierte unakzeptable Risiken der TBDS, die in Zusammenhang mit den vom IT-Service Provider für die TBDS erbrachten IT-Services stehen, eine mögliche Strategie und Maßnahmen zur Bewältigung der Risiken zu erarbeiten,
- unabhängige Bewertungen zur Verbesserung Informationssicherheit sicher zu stellen,
- selbst regelmäßig Management Reviews des Informationssicherheitsniveaus durchzuführen,
- das Sicherheitsniveau und dem Risiko angemessene Indikatoren zusammen mit TBDS zu definieren und regelmäßig an TBDS zu berichten,
- gesetzliche und behördliche Anforderungen und vertragliche Verpflichtungen zur Informationssicherheit zu identifizieren und zu behandeln,
- das Bewusstsein für die Sicherheit der IT-Services / IuK-Systeme der TBDS und die notwendigen Kompetenzen zu ermitteln und ggf. durch Schulungen zu fördern,
- interne und externe Kontaktstellen und Informationsquellen für die Informationssicherheit zu etablieren und zu kommunizieren,
- die in diesem Dokument aufgeführten Anforderungen für die „Konzeption“ und den „Betrieb“ von IuK-Systemen zu berücksichtigen

Die Umsetzung der zuvor aufgeführten Anforderungen muss im Sinne der Revisionssicherheit und etwaiger Haftungsansprüche belegbar dokumentiert werden.

Darüber hinaus sind IT-Service Provider der TBDS verpflichtet ein wirksames ***I***nformations- ***S***icherheits-***M***anagement-***S***ystem (ISMS) auf Basis ISO27001 zu etablieren, dieses aufrecht zu erhalten und kontinuierlich zu verbessern, insofern TBDS dies vertraglich als Anforderung definiert. Dies ist gegebenenfalls durch ein Zertifikat nachzuweisen.

4. Allgemeine Anforderungen an die IT-Service Provider der TBDS

- Unter Mitarbeiter sind nachfolgend die Beschäftigten des IuK- Service Provider zu verstehen.
- Der Verantwortungsbereich eines jeden Mitarbeiters mit Rechten zur Konfiguration von IuK- Systemen, welche zur Bereitstellung von IT-Services für die TBDS notwendig sind, muss in Hinblick auf die zu konfigurierenden informations- und kommunikationstechnischen Systeme und seine Kompetenzen (Rechte und Pflichten) definiert und dokumentiert sein.
- Die Fähigkeiten dieser Mitarbeiter müssen der Aufgabestellung der „Konfiguration, der in seinem Verantwortungsbereich liegenden IuK-Systeme“ entsprechen.
- Der Missbrauch von IuK-Systemen ist durch geeignete Aufgabentrennung durch den IT- Service Provider zu verhindern.

- Planung und Bereitstellung der für die Betriebssicherheit notwendigen Ressourcen
- Schaffen eines Bewusstseins der Mitarbeiter für die Bedeutung der Informationssicherheit für den TBDS Geschäftserfolg.
- Regelmäßige Durchführung einer Bedrohungsanalyse und Ermittlung und Dokumentation der Eintrittswahrscheinlichkeit (EW) und Auswirkungen auf die TBDS Informationswerte / IT- Services / IuK-Systeme hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität. Eine Bedrohungsanalyse ist in jedem Falle durchzuführen, sobald sich die Gefährdungslage ändert.

4.1. Anforderungen an die Einbindung in das Risikomanagement der TBDS

Das Risiko- und Chancen Management (RCM) ist in der TBDS einheitlich geregelt.

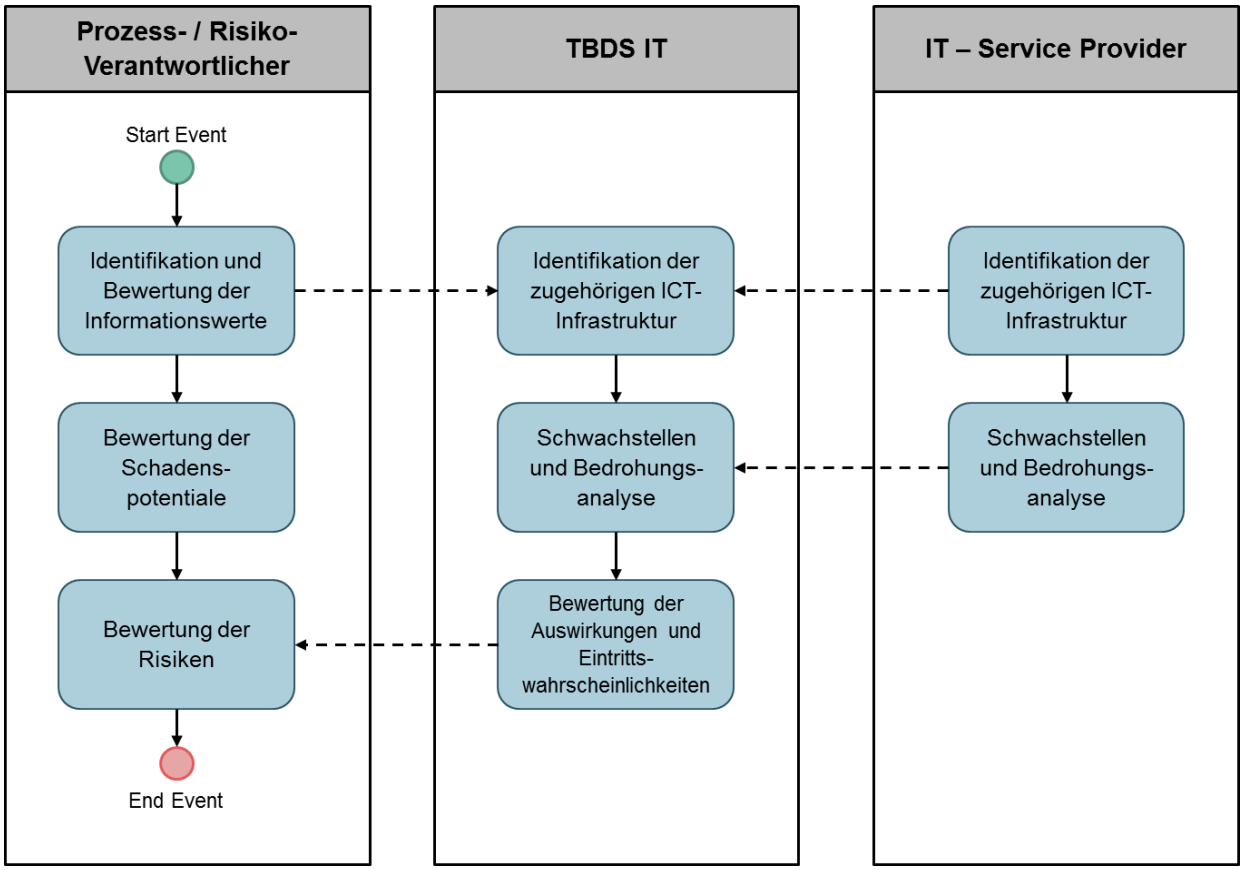
Ziel des RCM ist es, Risiken und Chancen (R&C) der betrieblichen Geschäftstätigkeit frühzeitig zu identifizieren, Konsequenzen der Übernahme zu erkennen, potentiell erfolgsentscheidende R&C zu steuern und existenzgefährdende Risiken zu vermeiden. Die sich daraus ergebende Aufgabenstellung im Hinblick auf Risiken umfasst die Erarbeitung und Umsetzung von Maßnahmen zur Risikobewältigung (Vermeidung, Verminderung, Abwälzung, Akzeptanz) unter Beachtung von Kosten / Nutzen- Aspekten.

In diesem Rahmen ist bei der Unterstützung der Geschäftsprozesse der TBDS durch Kommunikations- und Informationstechnik durch einen IT-Service Provider die Eintrittswahrscheinlichkeit für einen Verlust an Verfügbarkeit, Vertraulichkeit und Integrität bei der Datenverarbeitung, dem Datentransport und der Datenspeicherung anhand realistischer Bedrohungsszenarien zu ermitteln und den relevanten Gremien der TBDS mitzuteilen. Für die Brutto- und Nettobewertung der Risiken ist die Eintrittswahrscheinlichkeit von Schadenszenarien einmal ohne Berücksichtigung von Maßnahmen und einmal mit Berücksichtigung von Maßnahmen anzugeben.

Bei der Auswahl geeigneter IT-Sicherheitsmaßnahmen zur Bewältigung eines Risikos ist die TBDS IT und die TBDS Sicherheitsorganisation durch den IT-Service Provider einzubeziehen. Die Anforderungen aus dem TBDS Regelwerk der Informationssicherheit sind zu berücksichtigen und ggf. zu ergänzen, falls hiermit nicht das erforderliche Sicherheitsniveau zu erreichen ist.

Schon bei der Konzeption der Sicherheitsmaßnahmen ist auch auf die Messbarkeit der Wirksamkeit im Sinne der Belegbarkeit zu achten, um ggf. auch den Anforderungen des Internen-Kontroll-Systems (IKS) gerecht zu werden.

4.1.1. Prozessdarstellung



4.2. Anforderungen an die „Konzeption“ von TBDS IuK-Systemen

Zur Konzeption von IuK-Systemen existieren in der TBDS übergreifende Regelungen zur Informationssicherheit, welche nach der Vereinbarung einer Vertraulichkeitserklärung (NDA) dem Dienstleister, mit Bezug auf seine Aufgaben, zugänglich gemacht werden sollen. Darüber hinaus gilt allgemein:

- Der Entwurf und die Spezifikation von IuK-Systemen muss eine Bedrohungsanalyse beinhalten. Hierbei sind die Auswirkungen auf Informationswerte, IT-Services und IuK- Systeme zu berücksichtigen.
- Die Planung zukünftiger Kapazitätsanforderungen muss regelmäßig mit der TBDS abgestimmt werden und gegenwärtige und absehbare Trends berücksichtigen.
- Implementierungs-, Integrations- und Prüfkonzepte müssen die Ergebnisse der Risikoanalysen und der daraus resultierenden Behandlungspläne berücksichtigen. Hierbei ist auf die Unabhängigkeit der eingesetzten Prüfer zu achten, d.h. der Prüfer darf nicht an Entwurf, Spezifikation oder Planung der betroffenen IuK-Systeme beteiligt sein.
- Zu jedem IuK- System muss deren zulässige / vorgesehene Nutzung definiert werden.

- Bei der Konzeption von IuK-Systemen ist abhängig von den risikoorientierten Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität der Daten auf die physische und umgebungsbezogene Sicherheit des Aufstellungsortes zu achten.

  Dies sind:
  - Schutz vor Ausfall der Versorgungseinrichtungen (Energie und Kühlung) für informations- und kommunikationstechnische Systeme inkl. Management der Versorgungskapazitäten
  - Einbruchschutz – Maßnahmen zur Identifikation und Verhinderung des unberechtigten Zutritts zu und der Sabotage an informations- und kommunikationstechnischen Systemen
  - Zutrittsschutz – Verwaltung und technische Steuerung des Zutritts zu den informations- und kommunikationstechnischen Systemen inkl. Lieferbereiche
  - Brandschutz – Maßnahmen zur Identifikation und Verhinderung / Ausbreitung eines Brandes und der Beeinträchtigung durch Brandgase (Rauch) inkl. Löschanlagen und Entrauchung
  - Schutz vor Umgebungsgefahren – zum Beispiel Eindringen von (Lösch-)Wasser, Kapazitäten (Fläche, Energie, Kühlung), Erdbeben, Explosion, Feuer, Ansaugen von Rauchgasen, Überschwemmungen, Unruhen
  - Baulicher Schutz – Zum Beispiel Tragfähigkeit der Decken / Böden, Eignung der Transportwege und Verkehrsflächen
  - Raumluftkonditionierung – Luftwechselraten, Temperaturregelung, Luftfeuchteregelung
  - Schutz von Kabeln und Leitungen – Zum Beispiel gegen Abhören und Beschädigung
  - Betriebsbedingungen der Hersteller technischer Komponenten

- Auch die Entwickler und Tester stellen eine Bedrohung für die Vertraulichkeit betrieblicher Informationen der TBDS dar. Es muss daher ermittelt werden, ob eine Trennung von Produktions-, Test- und Entwicklungsumgebungen erforderlich ist, um unakzeptable Risiken für die TBDS Geschäftsprozesse zu vermeiden. Bei erforderlicher Trennung sind die folgenden Punkte zu berücksichtigen:
  - Die Regeln für den Übergang von Software aus der Entwicklungs- in die Produktionsphase müssen definiert und dokumentiert werden
  - Entwicklungs- und Produktionssoftware müssen auf verschiedenen Systemen oder Prozessoren und in unterschiedlichen Domänen oder Verzeichnissen laufen
  - Compiler, Editoren und sonstige Entwicklungswerkzeuge oder System- Dienstprogramme dürfen nicht von Produktionssystemen aus zugänglich sein, wenn dies nicht nötig ist
  - Die Testsystem-Umgebung sollte die Produktionssystem-Umgebung so genau wie möglich nachstellen
  - Benutzer sollten unterschiedliche Benutzerprofile für Produktions- und Testsysteme verwenden
  - Test- / Entwicklungssysteme sind so zu kennzeichnen, dass eine Identifikation des Systems gewährleistet ist und damit eine Fehlbenutzung weitestgehend ausgeschlossen wird
  - sensible Daten dürfen nicht in eine geringer als die Produktionsumgebung geschützte Testsystemumgebung kopiert werden

- Eine produktive Nutzung neuer Geräteklassen und Softwaretechnologien für die TBDS, darf nur nach erfolgreichen Implementierungs- und Integrationsprüfungen und nach Freigabe durch die zuständigen Gremien der TBDS erfolgen.
- Es ist auf eine formale Bestätigung der Sicherheitsmaßnahmen durch die zuständigen Gremien der TBDS zu achten.
- Für extern erreichbare Web-Anwendungen sind OWASP Top25 Prüfungen durchzuführen und die Ergebnisse an TBDS weiterzugeben.
- Die zentralen Messaging Systeme der TBDS sind so zu konzipieren, dass diese gegen DoS Attacken, Schadcode und Spam geschützt sind.
- Für die Benutzer der TBDS Messaging Systeme sind geeignete Verfahren zur Verschlüsselung von Nachrichten bereitzustellen.
- Bei der Konzeption von elektronischen Geschäftssystemen (e-Business) sind mindestens die folgenden Kriterien zu beachten:
    - Grad des Vertrauens, den jede Partei hinsichtlich der von der anderen angegebenen Identität fordert, z.B. durch Authentifizierung;
    - Berechtigungsprozesse hinsichtlich der Frage, wer zur Festsetzung von Preisen und zur Ausstellung oder Unterzeichnung von wichtigen Handelsdokumenten berechtigt ist;
    - Sicherstellung, dass die Handelspartner vollständig über ihre Berechtigungen informiert sind;
    - Bestimmung und Erfüllung der Anforderungen an Vertraulichkeit, Integrität, Versandnachweis und Erhalt wichtiger Dokumente sowie an die Nichtabstreitbarkeit von Verträgen, z.B. in Verbindung mit Angebotsabgabe- und Vertragsprozessen;
    - erforderlicher Grad des Vertrauens auf die Integrität veröffentlichter Preislisten;
    - Vertraulichkeit von sensiblen Daten oder Informationen;
    - Vertraulichkeit und Integrität aller Bestelltransaktionen, Zahlungsinformationen, Lieferadressangaben und Empfangsbestätigungen;
    - angemessener Grad der Überprüfung hinsichtlich der von den Kunden angegebenen Zahlungsinformationen;
    - Auswahl der am besten zum Schutz vor Betrug geeigneten Zahlungsform;
    - Grad des Schutzes, der erforderlich ist, um die Vertraulichkeit und Integrität von Bestellinformationen aufrechtzuerhalten;
    - Vermeidung von Verlust oder Duplizierung von Transaktionsinformation;
    - Haftungsverhältnisse im Zusammenhang mit betrügerischen Transaktionen;
    - Versicherungsanforderungen;
    - Einhaltung gesetzlicher Anforderung bei Anwendung von kryptographischen Maßnahmen

- Für alle IuK-Systeme der TBDS sind Berechtigungskonzepte zu erstellen. Es sind mindestens folgende Aspekte in den Berechtigungskonzepten zu berücksichtigen:
    - Sicherheitsanforderungen der TBDS an die relevanten IT-Services
    - Gesetze und jegliche vertraglichen Verpflichtungen hinsichtlich des Zugriffsschutzes für Daten oder Dienste
    - Die technische Umsetzung der Vergabe und des Entzuges von Rechten (technische Rechteverwaltung) und deren Zuordnung zu Personen
    - Das organisatorische Vergabeverfahren mit Antragstellung und Freigabe
    - Das organisatorische Rechtentzugsverfahren

- Die revisionssichere Dokumentation der aktuellen Berechtigungen und der Vergabe- und Entzugsverfahren
- Ein Prüfverfahren zur Feststellung der Ordnungsmäßigkeit der aktuellen Berechtigungen
- Verwaltung von Privilegien

4.2.1. Anforderungen an die „Konzeption“ von Netzwerkdiensten

- Für alle Netzwerke der TBDS sind Berechtigungskonzepte zu erstellen. Es sind mindestens folgende Aspekte in den Berechtigungskonzepten zu berücksichtigen:
  - Sicherheitsanforderungen der TBDS an die relevanten Netzwerkdienste
  - Gesetze und jegliche vertraglichen Verpflichtungen hinsichtlich des Zugriffsschutzes für Netzwerkdienste
  - Das organisatorische Vergabe- und Entzugsverfahren mit Antragstellung und Freigabe
  - Die revisionssichere Dokumentation der aktuellen Berechtigungen und der Vergabe- und Entzugs
  - Ein Prüfverfahren zu Feststellung der Ordnungsmäßigkeit der aktuellen Berechtigungen
  - Verwaltung von Privilegien für die Konfiguration von und den Zugriff auf Netzwerkkomponenten
  - Verwaltung der Netze und Netzdienste, auf die ein Zugriff gestattet ist
  - Maßnahmen und Verfahren des Managements zum Schutz des Zugriffs auf Netzverbindungen und Netzdienste inkl. des Fernzugriffs
  - die für den Zugriff auf Netzdienste angewendeten Mittel
  - Maßnahmen und Verfahren des Managements zum Schutz des Zugriffs auf Diagnose- oder Konfigurations-Ports
- Die Netzwerkinfrastruktur für TBDS ist so zu konzipieren, dass die Netze dem Risiko entsprechend nach unterschiedlichen Klassen/Bereichen getrennt werden (z.B. DMZ, Admin File, Admin SAP, SAP, Produktionssteuerung, etc.). Die Netzübergänge sind besonders zu schützen und für Benutzer zu beschränken.
- Es sind Routing-Kontrollen zu implementieren, die auf positiven Prüfmechanismen für Quell- und Zieladresse basieren.
- Remote-Zugriffe dürfen nur mittels starker Authentifizierung ermöglicht werden.

4.3. Anforderungen an den „Betrieb“ von TBDS IuK-Systemen

Zum Betrieb von TBDS IuK-Systemen existieren in der TBDS übergreifende Regelungen welche nach der Vereinbarung einer Vertraulichkeitserklärung (NDA) dem Dienstleister, mit Bezug auf seine Aufgaben, zugänglich gemacht werden sollen. Darüber hinaus gilt allgemein:

- IuK- Systeme, welche interne, vertrauliche oder streng Vertrauliche Informationen enthalten, müssen vor der Entsorgung entweder physisch zerstört oder die darauf gespeicherten Informationen vernichtet, gelöscht oder überschrieben werden. Dabei sind anstelle der einfachen Lösch- oder Formatierungsfunktion vorzugsweise Verfahren anzuwenden, welche die ursprünglichen Informationen nicht wiederherstellbar machen. Hierzu kann auch ein entsprechend spezialisiertes und vertraglich gebundenes Unternehmen eingesetzt werden. Bei beschädigten Geräten und Bauteilen, die sensible Daten enthalten, ist eine Risikobewertung erforderlich, um festzustellen, ob sie, anstatt in Reparatur gegeben oder ausrangiert zu werden, besser physisch zerstört werden sollten.

- Für die von der TBDS genutzten IuK- Systeme sind Dokumentationen zu erstellen, sodass bei einem Ausfall von Personal oder der Störung von Systemfunktionen schnellstmöglich der normale Betriebszustand wiederhergestellt werden kann.

Dazu gehören:

- Verarbeitung und Behandlung von Daten
- Backup
- Ablaufplanung
- Abhängigkeiten mit anderen IuK-Systemen
- Anweisungen für die Fehlerbehandlung oder den Umgang mit sonstigen Ausnahmebedingungen einschließlich Einschränkungen des Gebrauchs von Hilfsprogrammen
- Anlaufstellen für technische Unterstützung im Falle des Auftretens unerwarteter operativer oder sonstiger technischer Schwierigkeiten
- Neustart der Systeme und Wiederanlauf-Verfahren bei Systemausfall
- Management von Prüfspuren (Audit Trails) und Systemprotokoll-Informationen
- Systemspezifische Änderungsverfahren
- Definition von Verantwortlichkeiten

- Die Dokumentation der Systemkonfigurationen und Betriebsorganisation sind vor unberechtigtem Zugriff und Einsichtnahme zu schützen.
- Es ist ein dokumentiertes Verfahren zur Verwaltung von Änderungen (Change Management) zu definieren, dass einen möglichst geringen Einfluss von Änderungen an Informations- und kommunikationstechnischen Systeme auf die TBDS IT-Services gewährleistet. Die folgenden Punkte müssen im Änderungsverfahren berücksichtigt werden:
  - Feststellung und Aufzeichnung bedeutender Änderungen
  - Planung von Änderungen und Durchführung entsprechender Tests
  - Bewertung der potentiellen Risiken dieser Änderungen, einschließlich der Auswirkungen auf die TBDS IT-Services
  - formales Freigabeverfahren für vorgeschlagene Änderungen
  - Mitteilung der Details der jeweiligen Veränderungen an alle betroffenen Personen
  - Verfahren und Verantwortlichkeiten für den Abbruch von Änderungen
  - Wiederherstellung des Ausgangszustandes nach fehlgeschlagenen Änderungsversuchen und unvorhergesehenen Ereignissen (Rollback-Verfahren)
  - Regelung zum Umgang mit Notfall-Änderungen (Emergency Changes)

- Die Auslastung der Informations- und kommunikationstechnischen Systeme muss überwacht und mit den Sollwerten abgestimmt werden. Im Rahmen der Kapazitätsplanung müssen Abschätzungen angestellt werden, um die geforderte Systemleistung für die TBDS IT Services sicherzustellen.
- Neue Informationssysteme, Upgrades und neue Versionen dürfen nur nach einer formalen Freigabe in die Produktion übernommen werden. Bei der formalen Freigabe neuer Systeme müssen mindestens die folgenden Punkte Berücksichtigung finden:
- Nachweis der erforderlichen Leistungs- und Rechnerkapazität
  - Fehlerbehebungs-, Neustart- und Wiederanlaufverfahren
  - Vorbereitung und Test der Betriebsverfahren
  - Vollständigkeit der Sicherheitsmaßnahmen

- Kontinuitätsmanagement und Notfallpläne
- Nachweis, dass die Installation des neuen Systems bestehende Systeme nicht beeinträchtigt insbesondere zu Spitzenzeiten
- Schulung hinsichtlich des Betriebes und der Benutzung der neuen Systeme

- Es sind geeignete Vorkehrungen zur Abwehr von Schadsoftware zu treffen. Hierzu existieren in der TBDS übergreifende Regelungen welche nach der Vereinbarung einer Vertraulichkeitserklärung (NDA) dem Dienstleister, mit Bezug auf seine Aufgaben, zugänglich gemacht werden sollen.
- Für jedes Informations- und kommunikationstechnische System der TBDS muss ein Backup und Recovery Verfahren eingerichtet werden, das den folgenden Anforderungen entspricht:

Schnellst mögliche Wiederherstellung verlorener oder beschädigter Daten auf Anforderung sowie Auslagerung für den Katastrophenfall (BCM)	(1) Für jedes System müssen Vorgaben zur Datensicherung und -wiederherstellung im Rahmen eines Datensicherungskonzepts inkl. der verantwortlichen Personen definiert werden.
	(2) Sind Daten über verschiedene Systeme verteilt, ist übergeordnete Datenkonsistenz zu gewährleisten.
	(3) Bei lokaler oder mobiler Datenhaltung sind kritische Daten nur als Kopie, bzw. ausschließlich so lange wie erforderlich vorzuhalten und zu einer dauerhaften Dokumentenablage auf zentralen Systemen zu speichern.
	(4) Das Datensicherungskonzept ist mindestens einmal jährlich einer detaillierten Prüfung zu unterziehen. Das Ergebnis der Prüfung ist zu dokumentieren und als Nachweis aufzubewahren.
	(5) Für den Aufbewahrungsort der Datensicherungen müssen mindestens die gleichen Zutritts- und Zugriffsbeschränkungen gelten wie für die Systeme, auf denen die Originaldaten gespeichert sind. Weiterhin sind Maßnahmen zu treffen, welche die Datensicherungsmedien vor äußerlichen Einflüssen z. B. durch Feuer, Wasser, Diebstahl oder Sabotage schützen.
	(6) Die Datensicherungsmedien sind zu katalogisieren und regelmäßig auf ihre Vollzähligkeit und Lesbarkeit zu prüfen. Die Dokumentation muss revisionsfähig erfolgen.
	(7) Die Wiederherstellung geschäftskritischer Daten ist wenigstens einmal jährlich zu testen. Die durchgeführten Tests sind zu dokumentieren.
	(8) Besondere Maßnahmen sind bei verschlüsselten Daten oder Datenträgern zu etablieren.
	(9) Nicht mehr benötigte oder ausgetauschte Datenträger sind so zu vernichten, dass eine Rekonstruktion der gespeicherten Daten unmöglich ist.

- Darüber hinaus muss das Backup- und Recovery-Konzept folgende Punkte berücksichtigen:
  - es muss abhängig vom Risiko gemeinsam mit der TBDS festgelegt werden, für welche Informationen in welcher Ausprägung ein Backup erforderlich ist. Dies ist angemessen zu dokumentieren (z.B. SLA)
  - es müssen die gesetzlichen Aufbewahrungsfristen berücksichtigt werden
  - es müssen vollständige Aufzeichnungen über die Sicherungskopien unter Berücksichtigung einer nachvollziehbaren Kennzeichnung erstellt werden
  - der Umfang (z.B. vollständiges oder teilweises Backup) und die Frequenz des Backups muss die Geschäftsanforderungen der TBDS für den Normalbetrieb und abhängig vom betrieblichen Kontinuitätsmanagement (BCM) auch den Notfall widerspiegeln
  - Das Backup für die Notfallvorsorge muss abhängig vom betrieblichen Kontinuitätsmanagement in ausreichender Entfernung aufbewahrt werden, sodass dieses Backup nicht von der gleichen Katastrophe betroffen ist
  - Die Datenträger sind während des Transports zwischen den Standorten zu schützen (Übergabeverfahren, Verpackung, Transportmittel, zuverlässiger Botendienst)

- Es sind geeignete Betriebsverfahren festzulegen, um Datenträger (z.B. Bänder, Platten) gegen unberechtigte Weitergabe, Änderung, Entfernung und Vernichtung zu schützen. Dies gilt auch im Falle der Lagerung, Wartung und Reparatur.
- Bei der Entsorgung von Datenträgern ist darauf zu achten, dass vertrauliche Daten so zerstört werden, dass diese nicht wiederhergestellt werden können.
- Die Uhren aller TBDS IuK-Systeme müssen auf eine vereinbarte Referenzzeit synchronisiert werden. Falls ein Rechner oder eine Kommunikationseinrichtung über die Funktion einer Echtzeituhr verfügt, muss diese auf die einheitliche Referenzzeit eingestellt werden. Da einige Uhren bekanntlich mit der Zeit vor- oder nachgehen, muss ein Verfahren eingerichtet werden, das signifikante Abweichungen erkennt und korrigiert. Die richtige Einstellung von Rechneruhren ist wichtig, um die Genauigkeit von Auditprotokollen sicherzustellen, die für Ermittlungen oder als Beweise vor Gericht oder in Disziplinarverfahren erforderlich sein können. Ungenaue Auditprotokolle können solche Untersuchungen behindern und die Glaubwürdigkeit derartiger Beweismittel beeinträchtigen.
- Für alle TBDS IuK-Systeme müssen nachvollziehbare Prozesse zur Benutzerregistrierung und -deregistrierung existieren. Antragstellung, Freigabe und Entzug einer Berechtigung müssen dokumentiert werden. Dies gilt auch für die privilegierten Benutzer des IT-Service Providers.
- Allen Benutzern in den IuK-Systemen der TBDS muss eine eindeutige persönliche Benutzerkennung (User ID) zugewiesen werden. Durch die Authentisierungstechnik muss die vorgegebene Identität des Benutzers eindeutig bestätigt werden.
- Die TBDS IuK-Systeme sind (sofern technisch möglich) so zu konfigurieren, dass nur Passwörter akzeptiert werden, die den in der TBDS definierten Standardanforderungen genügen. Hierzu existieren in der TBDS übergreifende Regelungen welche nach der Vereinbarung einer Vertraulichkeitserklärung (NDA) dem Dienstleister, mit Bezug auf seine Aufgaben, zugänglich gemacht werden sollen.
- Bestehende Berechtigungen müssen in einem regelmäßigen Intervall überprüft werden. Die Intervalle zur Prüfung müssen dem Umfang und der Notwendigkeit der Zugriffsrechte Rechnung tragen. Die durchgeführten Prüfungen müssen nachvollziehbar dokumentiert werden. Die Dokumentation ist zu Nachweiszwecken sicher aufzubewahren.

- Bei allen TBDS IuK-Systemen ist der Zugriff auf Betriebssysteme durch ein ***sicheres*** Anmeldeverfahren zu schützen. Hierbei ist zu berücksichtigen, dass:
  - keine System- oder Anwendungskennungen anzeigt werden, bevor der Anmeldeprozess erfolgreich abgeschlossen wurde.
  - die Anmeldeinformationen ernst nach Beendigung aller Eingabedaten bestätigt werden. Falls ein Fehler auftritt, sollte das System nicht anzeigen, welcher Teil der Daten richtig oder falsch ist.
  - die Anzahl der erlaubten erfolglosen Anmeldeversuche und die zulässige Höchst- und Mindestdauer begrenzt wird.
  - Passwörter nicht im Klartext über das Netzwerk übertragen werden
  - Vorzugsweise sollte durch den Einsatz von Passwort Management Systemen sicher Passwörter erzwungen werden.

- Die Verwendung von Systemdienstprogrammen, die in der Lage sind, sich über System- und Anwendungseinstellungen hinwegzusetzen, ist Benutzern mit erweiterter Berechtigung (z.B. Systemadministratoren) vorbehalten. Der Einsatz ist zu Protokollieren und für andere Benutzer zu verhindern.
- Die TBDS IuK-Systeme sind so zu konfigurieren, dass inaktive Sessions nach einer festgelegten Dauer Inaktivität geschlossen werden.

4.3.1. Anforderung an den „Betrieb“ von Netzwerkdiensten

- Zum Schutz der internen und externen Kommunikation existieren in der TBDS übergreifende Regelungen welche nach der Vereinbarung einer Vertraulichkeitserklärung (NDA) dem Dienstleister, mit Bezug auf seine Aufgaben, zugänglich gemacht werden sollen.

  Darüber hinaus:
  - Müssen die Verantwortlichkeiten für den Netzbetrieb von der Verantwortlichkeit für den Rechnerbetrieb getrennt sein.
  - Sind die Sicherheitsmerkmale der Netzdienste zu definieren und zu dokumentieren
  - Darf Benutzern der direkte Zugriff nur auf solche Dienste ermöglicht werden, für deren Nutzung sie ausdrücklich durch die TBDS berechtigt wurden.
  - Ist zu ermitteln, welche Sicherheitsvorkehrungen, wie Sicherheitsmerkmale, Servicelevels und Managementanforderungen, für bestimmte Netzwerkdienste erforderlich sind. Es muss sichergestellt werden, dass die betreffenden Maßnahmen implementiert sind.

4.3.2. Anforderung an Administratoren der IT-Service Provider

Aufgrund ihrer besonderen Verantwortung beim Betrieb von IuK Systemen sind die folgenden zusätzlichen Regelungen für Administratoren zu beachten:

- Für die Verwendung und Handhabung von Administratoren Passwörtern ist zu beachten, dass diese einem besonderen Schutz unterliegen müssen. Administratoren sind regelmäßig mittels geeigneter Maßnahmen (z.B. Schulungen, Trainings, Anweisungen) auf die besonderen Risiken aufmerksam zu machen.
- Vorgaben zum Passwort Management sind zentral zu definieren und gemäß den Anforderungen sich entwickelnder Technologien regelmäßig zu bewerten. Die Verwaltung von Passwörtern muss nach dokumentierten Verfahren erfolgen.
- Privilegierte Benutzerkennungen dürfen nicht für die alltägliche Arbeit genutzt werden.
- Bestehende Zugangsberechtigungen müssen in einem regelmäßigen Intervall überprüft werden Die Intervalle zur Prüfung müssen dem Umfang und der Kritikalität der Zugriffsrechte Rechnung tragen (insbesondere bei Personalwechsel).
- Für Anwendungen in verschiedenen Sicherheitseinstufungen dürfen keine identischen administrativen Passwörter verwendet werden
- Serverkonsolen sind bei Nichtverwendung zu sperren