Datenschutz- und Datensicherheitskonzept am Zentrum für Quantitative Biologie

Fassung vom 24. April 2017

Dr. Sven Nahnsen, Matthias Seybold, Sven Fillinger

Hier kann man einen allgemeinen Einführungstext schreiben, zum Beispiel Motivation, Gesetzgebung und Ziele der Datensicherheitskonzepte am QBiC.

Änderungsnachweis

3. Juli 2014

Author(en): Dr. Sven Nahnsen
Neuerstellung und erste Fassung des Datenschutz- und Datensicherheitskonzepts

24. Juli 2017

Author(en): Dr. Sven Nahnsen, Matthias Seybold, Sven Fillinger
Layout Neuauflage, Aktualisierung von technischen Daten, Überarbeitung der Begriffsabgrenzung `Datenschutz` und `Datensicherheit`.

Inhaltsverzeichnis

Betrieb des Zentrums für Quantitative Biologie (QBiC)

Präambel

Das Quantitative Biology Center (QBiC) wurde 2011 als zentrale Einrichtung der Universität Tübingen und mit Zusammenarbeit der Medizinischen Fakultät Tübingen, sowie dem Max Planck Instituts für Entwicklungsbiologie gegründet. Der technische Betrieb von der QBiC Infrastruktur findet dabei am Zentrum für Datenverarbeitung (ZDV) der Eberhard Karls Universität Tübingen statt.

Dieses Handbuch beschreibt die konkrete Umsetzung der in § 9 Landesdatenschutzgesetz (LDSG) geforderten technischen und organisatorischen Maßnahmen zum Datenschutz bei automatiserter Verarbeitung personenbezogener Daten und zurdas Datensicherheitskonzept am QBiC.

Die nachfolgenden Ausführungen untergliedern sich in Erläuterungen zu datenschutzrechtlichen Begriffen sowie der Definition der Schutzmaßnahmen für die zentrale DV-Anlage, den Netzwerkkomponenten für den Zugang und den lokalen Anschluss.

1 Grundlagen eines Datenschutzkonzeptes gemäß LDSG

Die in diesem Datenschutzkonzept festgeschriebenen Maßnahmen sollen den Missbrauch und die Verfälschung von personenbezogenen Daten verhindern. Werden in öffentlichen Stellen selbst oder im Auftrag Daten dieser Art verarbeitet, so haben die für die Datenverarbeitung (DV) verantwortlichen Stellen gemäß § 9 (3) LDSG in der Fassung vom 2.April 2003 (GBl. S 648) technische und organisatorische Maßnahmen zu treffen, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten.
So ist zu gewährleisten, dass

- nur berechtigte Personen auf Datenbestände Zugriff haben (Vertraulichkeit),
- Daten bei der Verarbeitung nicht verfälscht werden (Integrität),
- Datenbestände reproduziert werden können (Verfügbarkeit).

Diese Ziele können erreicht werden durch:

- gebäudetechnische Maßnahmen (gebäudespezifische und räumliche Absicherung),
- hardwaretechnische Maßnahmen (Hardware-Passwortschutz, Schlösser etc.),
- softwaretechnische Maßnahmen (Software-Passwortschutz, Auditing etc.).

Aus o. g. Gesetzestext geht weiter hervor, dass solche Maßnahmen nur erforderlich sind, wenn „[...]der Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden Daten, in einem angemessenen Verhältnis zum Schutzzweck steht“(siehe LDSG §9 (2)). Es wird daher nachfolgend ein Konzept erarbeitet, welches ausgehend von den am meisten zu schützenden Datenbeständen einen für das gesamte DV System ausreichenden Grundschutz gewährleistet.

1.1 Definition der Maßnahmen gemäß § 9 LDSG

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, welche die in den folgenden Kapiteln definierten Kontrollvorgaben berücksichtigen.

1.1.1 § 9 (3) Nr. 1 : Zutrittskontrolle

Im Rahmen der Zutrittskontrolle ist Unbefugten der Zugang zu Datenverarbeitungsanlagen zu verwehren. Geeignete Maßnahmen sind dedizierte EDV- und Verteilerräume, verschlossene Diensträume sowie restriktive Schlüsselvergabe.

1.1.2 § 9 (3) Nr. 2 : Datenträgerkontrolle

Die Maßnahmen zur Datenträgerkontrolle sollen verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1.1.3 § 9 (3) Nr. 3 : Speicherkontrolle

Die Speicherkontrolle dient der Vermeidung von unbefugten Eingaben in den Speicher sowie Verhinderung unbefugter Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten.

1.1.4 § 9 (3) Nr. 4 : Benutzerkontrolle

Wird durch technische oder organisatorische Maßnahmen verhindert, dass Datenverarbeitungsanlagen (DVA) mit Hilfe von Einrichtungen zur Datenübertragung unberechtigt genutzt werden, so spricht man von Benutzerkontrolle.

1.1.5 § 9 (3) Nr. 5 : Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung einer DVA Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

1.1.6 § 9 (3) Nr. 6 : Übermittlungskontrolle

Ziel der Übermittlungskontrolle ist es, zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.

1.1.7 § 9 (3) Nr. 7 : Eingabekontrolle

Die Eingabekontrolle stellt sicher, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in ein Datenverarbeitungssystem (DVS) eingegeben worden sind.

1.1.8 § 9 (3) Nr. 8 : Auftragskontrolle

Die Auftragskontrolle impliziert, dass eine Verarbeitung von Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers durchgeführt werden kann.

1.1.9 § 9 (3) Nr. 9 : Transportkontrolle

Ziel der Transportkontrolle ist es, zu verhindern, dass sowohl bei der Übertragung als auch während des Transports von Daten auf Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

1.1.10 § 9 (3) Nr. 10 : Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

1.1.11 § 9 (3) Nr. 11 : Organisationskontrolle

Organisationskontrolle bedeutet, dass innerbehördliche und innerbetriebliche Organisationen so zu gestalten sind, dass sie den besonderen Anforderungen des Datenschutzes gerecht werden. Nachfolgend der Maßnahmenkatalog für den Betrieb von QBiC, differenziert nach zentralen Netzwerkkomponenten und Arbeitsstationen.

2 Technische Architektur von der QBiC Infrastruktur

Der technische Betrieb von QBiC im Zentrum für Datenverarbeitung geht von einer stringenten Konzeption aus, welche folgende Eckpunkte umsetzt:

1. Im Rahmen der DFG Exzellenzinitiatve wurde eine gemeinsame Infrastruktur für die Tübinger Core Facilities (QBiC, Lisa+, E-Science Center) beantragt. Diese Infrastruktur beinhalten Cluster Resourcen, sowie Server zur Datenspeicherung.
2. Die technische Infrastruktur von QBiC ist getrennt von den übrigen, vom ZDV betriebenen Systemen. Dies gilt auch für die völlig separierte Datenspeicherung und für einen eigenständigen Netzwerkbereiche: QBiC verwendet einen vom BelWü bereitgestellten separaten Adressbereich (zwei Class-C-Netze 196.193.22 und 196.193.23).
3. Alle acht betriebenen Instanzen von aDIS/BMS verfügen jeweils über vier technisch getrennte Systeme:
    a) Produktivsystem
    b) Identischer Spiegel des Produktivsystems jeweils am anderen Standort (asynchrone Datenbank-Replikation mit max. 200 ms Versatz, s. u.)
    c) Testsystem
    d) Schulungssystem
4. Zugriff auf die QBiC Hardware:
    a) Zur Administration haben mitarbeitende Personen im ZDV und des QBiCs wie unten ausgeführt Zugriff auf alle Systeme
    b) Kunden und Kooperationspartner des QBiC: Diese haben Zugriff über die Web-Schnittstelle, das QBiC Portal

3 Struktur des ZDV

Das ZDV ist das Rechenzentrum der Universität Tübingen und zugleich technischer Betreiber der QBiC Infrastruktur. Es versorgt bedarfsgerecht Studierende, Fakultäten und zentrale Einrichtungen mit einer IT-Infrastruktur und mit IT-Dienstleistungen, die Basis erfolgreichen Lernens, Lehrens und Forschens an der Universität Tübingen sind.

Das ZDV gliedert sich in fünf Abteilungen:

1. Campus IT Customer Services
2. Informations- und Verwaltungssysteme
3. Netze und Netzdienste
4. Personen- und Benutzermanagement
5. Zentrale Systeme

QBiC wird in der Abteilung Zentrale Systeme betrieben, für den Betrieb ist ferner die Mitarbeit der Abteilung Netze und Netzdienste notwendig.

3.1 Unterbringung des ZDV

Das ZDV verfügt über drei Gebäude und einen weiteren zentralen Serverbereich: 1. Hauptgebäude Wächterstraße 76 2. Gebäude Wilhelmstraße 106 3. Gebäude Rümmelinstraße 32 4. Serverraum Morgenstelle C2 5. Data Center, Auf der Morgenstelle xy

Die QBiC Hardware wird im zentralen Serverraum im Gebäude Wächterstraße 76Data Center, Auf der Morgenstelle xy, sowie im Serverraum Morgenstelle C2der Wächterstraße 76 betrieben; diese sind vollständig durch eine über die personalisierte Universitäts-Chipkarte gesteuertes Zugangskontrollsystem gesichert, Der Zugang zum Data Center ist zusätzlich per PIN gesichert..

Das Zugangskontrollsystem steuert den Zu- und Abgang zu den zentralen Serverräumen. Es wird ebenso protokolliert, wann welche Karte welche Operation auslöst.

Genaueres hierzu ist in der Ergänzung „Datenschutz- und Datensicherheitskonzept für den Betrieb der QBiC Infrastruktur – Unterbringung im Zentrum für Datenverarbeitung (ZDV) der Universität Tübingen“ ausgeführt.

4 Datenschutzkonzept

Hier sollten wir erklären, welche personenbezogenen Daten anfallen und wofür sie gebraucht werden. Anschließend dann alle Punkte nach LDSG §9 durchgehen und benennen, welche Maßnahmen wir zur Gewährleistung dieser Punkte ansetzen.

4.1 Begründung zur Sammlung personenbezogener Daten

Wir müssen an dieser Stelle kurz erwähnen, warum wir personenbezogene Daten verwenden. LDSG §3 macht dazu Angaben, auf die wir uns beziehen können.

4.2 Maßnahmen zur Wahrung des Persönlichkeitsrechts nach LDSG §9 (3)

Dieser Abschnitt wird sich mit der Datensicherheit überschneiden. Allerdings müssen wir an dieser Stelle aufführen, wie wir konkret die Maßnahmen durchsetzen, die vom LDSG gefordert sind.

5 Datensicherheitskonzept

Hier kommen Details für das Sicherheitskonzept, also wie wir im Allgemeinen mit Daten umgehen, Speichern und den Zugang kontrollieren.

5.1 Schutzmaßnahmen für die zentrale Rechnersysteme und Netzwerkeinrichtungen

Als zentrale Rechnersysteme und Netzwerkeinrichtungen werden solche Komponenten bezeichnet, die der zentralen Speicherung oder Übermittlung von Daten dienen. Dies sind insbesondere Server, Datenverteiler (Repeater, Bridges, Router), Firewalls und die Verkabelung. Diese sind grundsätzlich als besonders sicherheitskritisch anzusehen.

5.1.1 Server zum Betrieb von QBiC

Zu den Zielen von QBiC gehört die hochverfügbare Bereitstellung des zentralen webbasierten Zugangs, das QBiC Portal und die damit verbundenen OpenBIS Server zum Data Management. Um diese Hochverfügbarkeit zu erreichen, werden zwei parallele Servercluster jeweils bestehend aus 16 Blade-Systemen und zwei Storage-Clustersystemen an den Standorten Wächterstraße 76 und Morgenstelle C2im Data Center, Auf der Morgenstelle xy betrieben.

Applikations- und Datenbank-Server
Für die Bereitstellung der Fachanwendungen werden Server mit Betriebssystem Redhat Enterprise betrieben für die Funktionen:

- OpenBIS Applikationsserver zusammen mit Apache-Webserver und Tomcat Applikationsserver der gUSE/WS-PGrade Installation
- OpenBIS DataStoreServer (DSS): Datenbank-Server (Postgres)

Die Datenhaltung erfolgt auf Servern unter Betriebssystem Redhat Enterprise LINUX mit einheitlichen Versions-Ständen, auf denen jeweils das Datenbankmanagementsystem Postgres installiert ist. Der Portal Server besitzt zusätzlich eine MariaDB Installation.

Die aktuell verwendeten Versionen, Gerätebezeichnungen, Adressräume und die Patchstände der Betriebssysteme,, die Systeme und Anwendungen sowie die Spezifikationen für Serverhardware und Netzwerkeinbindung der Server werden in der ZDV-internen QBiC-Versionsdatenbank verwaltet. Sicherheitsupdates werden auf allen Systemen regelmäßig eingespielt.

5.1.2 § 9 (3) Nr. 2 : Datenträgerkontrolle

Die QBiC Hardware verwendet für die persistente Datensicherung an jedem Standort jeweils zwei Storageclustern vom Typ HP P4300 jeweils bestehend aus 16 32 Platten. Die einzelnen Datenträger (Festplatten) sind in den Gehäusen der P4300 montiert. Eine Reparatur erfolgt hausintern durch oder unter der Aufsicht eines Systemadministrators. Defekte Plattenlaufwerke sind physisch zu zerstören. Die endgültige Entsorgung erfolgt zusammen mit datenschutzrelevanten Papieren über ein beauftragtes Unternehmen. Das Unternehmen ist für die Entsorgung zertifiziert gem. der Ausschreibung der Zentralen Verwaltung.

Beide Betriebsstandorte spiegeln ihre Daten jeweils auf den anderen Standort asynchron (täglich) über Werkzeuge desLVM Snapshots. Zweimal wöchentlich (Sonntag, Mittwoch) wird per rsync die Daten des DSS synchronisiert. DBMS Postgres, wobei der maximale Versatz unter 200 ms liegt.

Zusätzlich erfolgt jede Nacht ein vollständiger Datenbank-Backup, der auf ein separates Storagesystem (Eurostore) gesichert wird. Die täglichen Transaktionen werden im laufenden Transaktions-Log im lokalen File-System gespeichert.

5.2 Datensicherung

Die Datensicherung erfolgt wie oben beschrieben Jede Nacht werden LVM Snapshot von den Produktivsystemen gemacht und auf den Backupserver übertragen. Zweimal wöchentlich findet eine Synchronisation zum Backupserver statt. durch asynchrone Datenbankreplikation jeweils an den zwei Standorten Wächterstraße und Morgenstelle, wobei der maximale Versatz unter 200 ms liegt; tägliches Datenbank-Dump auf getrenntes Storage-System; zwischen den DB-Dumps durch Aufzeichnung der Transaktions-Logs.

5.3 Schutzmaßnahmen für Applikations- und Datenbankserver

5.3.1 § 9 (3) Nr. 3 : Speicherkontrolle

Der administrative Zugang zu den IBS-Systemen ist durch folgende Maßnahmen vor unbefugten Eingaben geschützt:

1. Die einzelnen Server sind mit einem Zugangspasswort geschützt.
2. Der Zugang zu allen Servern ist durch Firewall-Regeln beschränkt:
   - Einzig möglicher Zugang über SSH
   - Nur SSH-Zugang von authorisierten Rechnern
   - Zugriff ist instanzenweise geregelt (vgl. 3)
   - Zugang über den User `root` ist nur für ausgewählte mitarbeitenden Personen des ZDV/QBiC möglich

- Zum Schutz vor „Brute Force“-Attacken verhindert eine laufende fail2ban Installation auf jedem System durch wiederholte fehlgeschlagene Logins per ssh
- Der Administrator wird per E-Mail über Attacken informiert

3. Die Konsolensitzung ist unmittelbar nach Beendigung von Arbeiten an der Konsole zu beenden, oder wenn erforderlich bei einer weiter aktiven Sitzung der Passwortschutz zu reaktivieren.

Das Passwort ist folgendem Personenkreis bekannt:
Zugang Systemadministrator einschl. Blade-Onboard-Administration Dr. Werner Dilling Dr. Ulrich HahnSven Fillinger Matthias Seybold Andreas Keck René Lange Timo VeithVolker Lutz Dr. Werner Dilling Dr. Ulrich Hahn Wer sonst noch vom ZDV Enrico Tagliavini

Folgende Funktionen/Rollen sind technisch für QBiC eingerichtet: Systemadministrator (s.o.) instanzenweiser Zugang auf Applikationsserver zum Starten/Beenden des Apache und des Tomcat instanzenweiser Zugang zum Datenbankserver zur Administration der Postgres-Datenbank Zugang zur Konsole des Storage-Systems: Wie oben Systemadministration

eingeschränkter Zugang Applikationsserver Sven Fillinger Matthias Seybold Andreas Friedrich Christopher Mohr Aydin Can Polatkan Dr. Stefan Czemmel Dr. Marius Codrea Dr. Erhan Kenar Wer sonst noch vom QBiC? Dr. Werner Dilling René Lange Andreas Keck Timo Veith Enrico Tagliavini

Zugang Datenbankserver Sven Fillinger Matthias Seybold Andreas Friedrich Christopher Mohr Aydin Can Polatkan Dr. Stefan Czemmel Dr. Marius Codrea Dr. Erhan Kenar Wer sonst noch vom QBiC? Dr. Werner Dilling René Lange Andreas Keck Timo Veith Enrico Tagliavini

Zugang Storage-System Dr. Werner Dilling Dr. Ulrich Hahn Matthias Seybold Sven Fillinger Volker Lutz Wer sonst vom ZDV?Andreas Keck René Lange Timo Veith Enrico Tagliavini

Administrative Arbeiten werden in den System-Logfiles protokolliert (ca. 3 Monate). Die System-Logfiles werden nach 90 Tagen gelöscht.

Diese Logfiles werden auf den einzelnen Serversystemen lokal gespeichert., eine systematische Zusammenführung durch den IBS-Manager steht unmittelbar bevor.

3.4.2 § 9 (3) Nr. 4 : Benutzerkontrolle

QBiC unterscheidet wie in 3 aufgeführt fünf Arten von Benutzern, die Zugang zu dem System haben. Für diese einzelnen Gruppen gelten verschiedenen Anforderungen und Regelungen für den Zugang bis hin zum weltweiten SSL-Verschlüsselten Zugang für Nutzende der Infrastruktur.

Die Authentifizierung der Nutzer erfolgt durch einen eigens dafür eingerichteten LDAP Server. Der QBiC LDAP Server wird vom ZDV verwaltet.

Für alle Zugriffe sind lokale Firewall-Regeln implementiert, die auf der Basis von Whitelists nur für dedizierte Adressen den jeweiligen Zugang ermöglichen.

Alle Zugriffe auf das System des QBiCs erfolgen verschlüsselt (TLS, SSH).

3.4.2.1 Administration: Mitarbeiter des ZDV/QBiC Für mitarbeitendes Personal des ZDV und des QBiCs besteht Zugang zu den Systemen wie oben beschrieben.

Kunden und Kooperationspartner des QBiCs greifen über ein Web-Frontend auf den Applikationsserver zu, wobei diese Zugriffe stets verschlüsselt erfolgen (TLS).

3.4.2.2 Passwortschutz Der Passwortschutz für administrative Zugänge unterliegt folgenden, vom ZDV vorgegebenen Regularien:

Die Mindestlänge beträgt 8 Zeichen. Aus mindestens 3 der folgenden 4 Kategorien muss ein Zeichen im Passwort enthalten sein: Kleinbuchstaben: a, b, c... Großbuchstaben: A, B, C... Ziffern: 1, 2, 3...

3.4.3 § 9 (3) Nr. 5 : Zugriffskontrolle

Das Landesprojekt IBS BW trennt die unter 3 beschriebenen acht Instanzen im technischen Betrieb; alle Zugänge sind auf die jeweiligen Instanzen beschränkt.

Für alle Zugriffe sind lokale Firewall-Regeln implementiert, die auf der Basis von Whitelists nur für dedizierte Adressen den jeweiligen Zugang ermöglichen. Ausgenommen davon ist der Zugang über den OPAC, welcher explizit weltweit für Recherchen freigeschaltet wurde.

3.4.4 § 9 (3) Nr. 6 : Übermittlungskontrolle

Die Übertragung von Daten kann nur durch authorisierteautorisierte Benutzer durchgeführt werden.

Alle diese Datenübertragungen erfolgen ausschließlich verschlüsselt.

3.4.5 § 9 (3) Nr. 7 : Eingabekontrolle Aufgrund der oben beschriebenen Maßnahmen ist eine unbefugte Eingabe von Daten nicht möglich.

Die adminstrativen Zugriffe werden (s.o.) protokolliert. Alle Transaktionen innerhalb des QBiC Portals werden innerhalb der Applikation protokolliert.

3.4.6 § 9 (3) Nr. 9 : Transportkontrolle 3.4.7 Die Server kommunizieren mit den Arbeitsstationen nur über gesicherte IP-Verbindungen (TLS, SSH). Ungesicherte Verbindungen sind nicht möglich. Die Übertragung von Passwörtern über das Netzwerk erfolgt prinzipiell in verschlüsselter Form.

Ein mechanischer Transport von Daten findet nicht statt.

3.4.8 § 9 (3) Nr. 10: Verfügbarkeitskontrolle 3.4.9 Die Benutzerberechtigungen werden so vergeben, dass versehentliches Löschen so weit möglich, ausgeschlossen ist. Über die tägliche Datensicherung, welche 14 Tage zurück reichen, wird ferner sichergestellt, dass versehentlich gelöschte oder zerstörte Daten wieder hergestellt werden können.

3.4.10 § 9 (3) Nr. 11: Organisationskontrolle

Die beteiligten Personen wurden mündlich über die Auswirkungen dieses Handbuches informiert und sind auf den Datenschutz verpflichtet. Dies erfolgte im Rahmen der förmlichen Verpflichtung bei der Einstellung von mitarbeitenden Personen bzw. im Zusammenhang mit dem Inkrafttreten des ersten Landesdatenschutzgesetzes. Über die förmliche Verpflichtung wurde im Rahmen der Einstellung ein Protokoll gefertigt.

3.5 Schutzmaßnahmen Netzwerkkomponenten Innerhalb des ZDV ist der Zugang und der Zugriff auf die aktiven Netzkomponenten auf folgende Personen beschränkt:

Mitarbeiter der Abteilung Zentrale Systeme, welche Zugriff auf Komponenten von QBiC haben (s.o.): Dr. Werner Dilling Dr. Ulrich Hahn Enrico Tagliavini 4. Andreas Keck René LangeVolker Lutz Sonst ZDV? Matthias Seybold Sven Fillinger

Mitarbeiter der Abteilung Netze und Netzdienste sowie Zentrale Systeme, die Zugriff auf die aktiven Netzkomponenten direkt an den Serversystemen (Blade-Switche) haben: Dr. Werner Dilling Andreas Keck Enrico Tagliavini René Lange Andreas Müller Jürgen RenzVolker Lutz Sonst ZDV? Matthias Seybold Sven Fillinger

Mitarbeiter der Abteilung Netze und Netzdienste, die Zugriff auf aktive Netzkomponenten haben, die von QBiC genutzt werden: Dr. Heinrich Abele Andreas Müller Jürgen Renz Rudi Seiz

Mitarbeiter des BelWü, die Zugriff auf die Tübinger BelWü-Router haben: Wolfram Hellstern Peter Merdian Tim KleefassWer? 5. Schutzmaßnahmen für Arbeitsstationen

Die nachfolgend aufgeführten Schutzmaßnahmen beziehen sich ausschließlich auf die Arbeitsplätze des ZDVQBiC, also für administrative Aufgaben am Kernsystem.

5.1 § 9 (3) Nr. 1 : Zutrittskontrolle

Alle Arbeitsplätze im ZDV QBiC sind über die personenbezogene Universitäts-Chipkarte und mechanischeelektronische Schlüssel geschützt.

5.2 § 9 (3) Nr. 2 : Datenträgerkontrolle

Mitarbeitende Personen des ZDV QBiC speichern auf ihren lokalen Arbeitsplatzgeräten keine QBiC-bezogenen Daten.

5.3 § 9 (3) Nr. 3 : Speicherkontrolle

siehe oben 5.4 § 9 (3) Nr. 4 : Benutzerkontrolle

siehe oben

5.5 § 9 (3) Nr. 5 : Zugriffskontrolle

Für die Mitarbeiter des ZDV QBiC gelten die oben beschriebenen Regularien für den Zugriff auf die QBiC-Systeme.

5.6 § 9 (3) Nr. 6 : Übermittlungskontrolle

Von QBiC werden keine Daten zur Speicherung auf Arbeitsplatzstationen der zuständigen mitarbeitenden Personen im ZDV übertragen.

5.7 § 9 (3) Nr. 9 : Transportkontrolle Die Arbeitsstationen kommunizieren mit den Servern nur über gesicherte IP-Verbindungen (IPSec ssh - Tunnel). Weitere Transporte finden nicht statt. 5.8 § 9 (3) Nr. 10 : Verfügbarkeitskontrolle Die Benutzerberechtigungen werden so vergeben, dass versehentliches Löschen so weit möglich, ausgeschlossen ist. Über die oben beschriebene Datensicherung wird sichergestellt, dass versehentlich gelöschte oder zerstörte Daten wieder hergestellt werden können. 5.9 § 9 (3) Nr. 11 : Organisationskontrolle

Die Maßnahmen zur Organisationbskontrolle für die mitarbeitenden Personen im ZDV QBiC sind oben bereits beschrieben.

6. Datenbestand

Die Erfassung, Änderung und Löschung von Daten innerhalb des DataStoreServers erfolgt ausschließlich durch die mit den entsprechenden Zugriffsrechten ausgestatteten mitarbeitenden Personen des QBiCs.

6.1 Art der Datenbestände

Die Datenbestände werden entsprechend ihrer Schutzbedürftigkeit innerhalb eines zweistufigen Schutzklassenmodells eingeordnet. Dabei ist die Zuordnung zu den Schutzklassen gemäß IuK-Rahmen-Dienstvereinbarung und DFN-Vorgaben zusammengefasst.

Die dort verwendeten Schutzklassen A und B sind unter A, die Klassen C und D unter B subsumiert.

Die Schutzmaßnahmen innerhalb des Gesamtsystems beziehen sich aber immer auf die höchste Schutzstufe. Eine Differenzierung nach unterschiedlichen Datenarten findet nicht statt.

Die Klassifikation der Datenbestände erfolgt deshalb auch nur der Vollständigkeit halber. 6.1.1 Schutzklasse A In Schutzklasse A werden personenbezogene Daten eingestuft, deren Missbrauch keine besondere Beeinträchtigung des Betroffenen erwarten lässt. Dies sind insbesondere die in § 15 (2) Nr. 7 LDSG aufgeführten „Daten aus allgemein zugänglichen Quellen...“. 6.1.2 Schutzklasse B Mit Schutzklasse B werden personenbezogene Daten bewertet, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen oder erheblich beeinträchtigen kann bzw. Daten die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Dies sind insbesondere Daten nach § 33 (1) LDSG sowie Daten, die auf schulische Leistungen Arbeitsverhältnisse Geschäftsbeziehungen Mietverhältnisse schließen lassen.

QBiC verfügt nur über Datenbestände der Schutzklasse A und B.

7. Datensicherung

Die Datensicherungsmaßnahmen für QBiC sind oben beschrieben. Sie bestehen im Wesentlichen aus:

1. Redundante Datenhaltung an zwei getrennten Standorten mit asynchroner Replikation, wobei die Replikationszyklen unter 200 ms liegen; 2. Tägliche LVM Snapshots der Produktivsysteme; zweimal wöchentliche Synchronisierung der Data Store Server s Datenbank-Backup auf getrenntes Speichermedium und Archivierung für 14 Tage; 3. Aufzeichnung der täglichen Backups werden per E-Mail am dem Administrator gesendet.

7.1 Lokale Firewalls Wie beschrieben sind alle Server-Systeme von QBiC über lokale Firewall, basierend auf IPTables, zusätzlich zu den allgemeinen Maßnahmen im Kommunikationsnetz der Universität Tübingen geschützt.

Die lokalen Firewalls basieren auf Whitelists, alle eingehenden Zugriffe (Adressen) müssen einzeln erlaubt werden: Für alle Zugriffe sind lokale Firewallregeln implementiert, die auf der Basis von Whitelists nur für dedizierte Adressen den jeweiligen Zugang ermöglichen.