DOLPHIN
an F24 company

# Datensicherheit
## und Datenschutz

| | |
|---|---|
| Dateiname | Dolphin Systems-Datensicherheit.docx |
| Version | 1.0 |
| Änderungsdatum | 25.10.2017 |

**DOLPHIN Systems AG**
Samstagernstrasse 45
8832 Wollerau
Schweiz

DOLPHIN
an F24 company

# Inhalt

# 1. Einleitung

In unserer vernetzten Welt bedarf das Thema Datenschutz und Datensicherheit grösster Sorgfalt. In diesem Dokument wird ausführlich auf den Datenschutz und die Datensicherheit bei Dolphin Systems eingegangen. Dieses Dokument gilt als Grundlage für alle von Dolphin Systems angebotenen Services und Dienstleistungen.

Datenschutz und Datensicherheit ist nicht das gleiche, daher sollen die beiden Begriffe an dieser Stelle kurz erklärt werden. Datenschutz ist der Schutz einer Person vor Beeinträchtigungen ihrer Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten, die sie betreffen. Datensicherheit ist ein Teil der Informationssicherheit, welche das Ziel verfolgt, Vertraulichkeit, Verfügbarkeit und Integrität sämtlicher Informationen permanent zu gewährleisten. Datensicherheit ist somit der umfassendere Begriff. Aus Gründen der besseren Lesbarkeit wird in diesem Dokument der Begriff Datensicherheit bevorzugt verwendet und soll den Datenschutz als Teil dessen mit einbeziehen.

Die Erbringung der Datensicherheit ist nicht nur das Einhalten der gesetzlichen Bestimmungen, sondern viel mehr eine ethische Haltung und leitet sich daher auch von der Unternehmensphilosophie ab. Daneben gibt es verschiedenste Anforderungen aus der Informationssicherheit, welche gedeckt sein müssen. Daraus lassen sich die Ziele in Bezug auf die Datensicherheit definieren.

Im Hauptteil dieses Dokuments werden die zentralen Massnahmen für die Erbringung der Datensicherheit bei Dolphin Systems beschrieben. Diese Massnahmen bestehen zum einen aus technischen Massnahmen und zum anderen aus organisatorischen Massnahmen.

Dolphin Systems ist stets darum bemüht, alle nötigen Anstrengungen und Vorkehrungen zu treffen, um ein Höchstmass an Datensicherheit zu erreichen.

# 2. Ausgangslage

Die Ausgangslage für sämtliche Überlegungen und Anstrengungen hinsichtlich der Datensicherheit bei Dolphin Systems bilden die folgenden drei Punkte:

- Unternehmensphilosophie
- Gesetzliche Vorschriften
- Informationssicherheit

Damit lassen sich anschliessend die Ziele hinsichtlich der Datensicherheit definieren.

## *2.1 Unternehmensphilosophie*

Für die Erbringung der Datensicherheit genügt es nicht, nur die gesetzlichen Vorschriften einzuhalten, sondern es braucht viel mehr eine ethische Haltung zur konsequenten und umfassenden Abdeckung aller sicherheitsrelevanten Risiken. Dolphin Systems sieht Datensicherheit als ein wesentliches Qualitätsmerkmal unserer Dienstleistung.

Gerade in unserer Branche ist es eine unternehmerische Verantwortung, ein hohes Mass an Sicherheit im Umgang mit Daten anzustreben. Aufgrund unserer langjährigen Zusammenarbeit mit Polizei, Feuerwehr, Spitälern, Banken und Gemeinden, welche zusätzliche Anforderungen an die Datensicherheit stellen, sind wir uns dieser Problematik nicht nur bewusst, sondern es gehört zu unserer täglichen Arbeit, damit umzugehen.

Wir bieten unseren Kunden ein Höchstmass an Sicherheit. Wenn es um die Datensicherheit geht, sind keine Kompromisse erlaubt. Wir sind uns bewusst, dass die Datensicherheit nur gewährleistet werden kann, wenn wir uns laufend über neue Erkenntnisse diesbezüglich informieren und unsere Prozesse laufend daran anpassen. Datensicherheit betrifft nicht nur einzelne Bereiche eines Unternehmens, sondern erstreckt sich über die gesamte Unternehmung hinweg.

## *2.2 Gesetzliche Vorschriften*

Neben unserer Unternehmensphilosophie gilt es, auch die vom Gesetz geforderten Vorschriften einzuhalten. Daher soll an dieser Stelle auch auf die zentralen Punkte des Bundesgesetzes über den Datenschutz (DSG) eingegangen werden. Das DSG bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

***Art. 7 Datensicherheit***

*1 Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.*

*2 Der Bundesrat erlässt nähere Bestimmungen über die Mindestanforderungen an die Datensicherheit.*

*Im Abschnitt 4 Technische und organisatorische Massnahmen der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) werden diese Massnahmen etwas genauer erläutert.*

***Art. 8 Allgemeine Massnahmen***

*1 Wer als Privatperson Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten, um einen angemessenen Datenschutz zu gewährleisten. Insbesondere schützt er die Systeme gegen folgende Risiken:*

- *a. unbefugte oder zufällige Vernichtung;*
- *b. zufälligen Verlust;*
- *c. technische Fehler;*
- *d. Fälschung, Diebstahl oder widerrechtliche Verwendung;*
- *e. unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.*

*2 Die technischen und organisatorischen Massnahmen müssen angemessen sein. Insbesondere tragen sie folgenden Kriterien Rechnung:*

- *a. Zweck der Datenbearbeitung;*
- *b. Art und Umfang der Datenbearbeitung;*
- *c. Einschätzung der möglichen Risiken für die betroffenen Personen;*
- *d. gegenwärtiger Stand der Technik.*

*3 Diese Massnahmen sind periodisch zu überprüfen.*

***Art. 9 Besondere Massnahmen***

*1 Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:*

*a. Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;*

*b. Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;*

*c. Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;*

*d. Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;*

*e. Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;*

*f. Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;*

*g. Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;*

*h. Eingabekontrolle: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.*

*2 Die Datensammlungen sind so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können.*

## 2.3 Informationssicherheit

Der dritte Punkt, der einen Einfluss auf die Ziele hat, ist die Informationssicherheit. Als Informationssicherheit bezeichnet man die Eigenschaften von informationsverarbeitenden Systemen, welche die Vertraulichkeit, Verfügbarkeit und Integrität gewährleisten. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken. Informationssicherheit bezieht sich auf alle relevanten Informationen einer Organisation oder eines Unternehmens einschliesslich personenbezogener Daten.

### 2.3.1 Vertraulichkeit

Vertrauliche Informationen müssen vor unbefugtem Zugang geschützt werden. Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung. Vertraulichkeit kann erreicht werden, wenn eine restriktive Beschränkung des Informationszugangs auf berechtigte Nutzer eingesetzt wird.

### 2.3.2 Verfügbarkeit

Systemausfälle müssen während der gesamten Betriebsdauer vermieden werden. Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zu einem beliebigen Zeitpunkt zur Verfügung. Es muss sichergestellt werden, dass der Zugang zu den Systemen jederzeit gewährleistet ist.

### 2.3.3 Integrität

Informationen dürfen nicht unbemerkt verändert oder manipuliert werden. Die Korrektheit (Unversehrtheit) von Daten ist für eine korrekte Funktionsweise von Systemen von zentraler Bedeutung. Daher muss die Integrität der Daten stets gesichert sein. Änderungen der Daten sollten später nachvollziehbar sein und daher festgehalten werden.

## *2.4 Ziele*

Sowohl aus der Unternehmensphilosophie als auch aus den gesetzlichen Vorschriften und den Erkenntnissen aus der Informationssicherheit lassen sich nun die Ziele im Zusammenhang mit der Datensicherheit definieren. Grundsätzlich geht es um die folgenden drei Ziele:

- Einhaltung der gesetzlichen Bestimmungen
- Erfüllung der Unternehmensphilosophie
- Gewährleistung der Informationssicherheit

Im Folgenden sollen die Ziele etwas ausführlicher und fassbarer beschrieben werden.

### *2.4.1 Einhaltung der gesetzlichen Bestimmungen*

Ein primäres Ziel ist es, jederzeit, ausnahmslos und vollumfänglich die gesetzlichen Bestimmungen gemäss dem Bundesgesetz über den Datenschutz (DSG) und der dazu gehörenden Verordnung VDSG einzuhalten.

### *2.4.2 Erfüllung der Unternehmensphilosophie*

Die Sensibilisierung der Mitarbeitenden hinsichtlich der Einhaltung rechtlicher und betrieblicher Vorgaben betreffend Informationssicherheit ist der zentrale Ansatz für die Umsetzung der Massnahmen. Für die Erbringung unserer Dienstleistungen und Services ist eine sehr hohe Datensicherheit unabdingbar. Daher ist ein weiteres Ziel, dass die von Dolphin Systems gepflegte Unternehmensphilosophie befolgt und gelebt wird.

### *2.4.3 Gewährleistung der Informationssicherheit*

Das Sicherstellen eines hohen Masses an Vertraulichkeit, Verfügbarkeit und Integrität sämtlicher im Einsatz stehenden Systeme und damit die Erbringung der Informationssicherheit ist das dritte Ziel. Dazu gehört die periodische Überprüfung der Wirksamkeit der getroffenen Sicherheits- und Schutzmassnahmen, Auswertung der Ergebnisse und regelmässige Anpassung der entsprechenden Massnahmen.

# 3. Massnahmen

In diesem Teil wird ausführlich auf die von Dolphin Systems ergriffenen Massnahmen eingegangen. Grundsätzlich lassen sich diese in technische und organisatorische Massnahmen gliedern.

## *3.1 Technische Massnahmen*

An dieser Stelle werden die bei Dolphin Systems im Einsatz stehenden technischen Massnahmen beschrieben.

### *3.1.1 Systemarchitektur der Rechenzentren*

Unsere Strategie ist, jedes System mindestens in doppelter Ausführung zu betreiben, so dass bei einer Störung oder einem Ausfall eines Systems mindestens ein Ersatzsystem zu Verfügung steht. Dies zeigt sich vor allem in der Architektur unserer Rechenzentren. Die zwei Rechenzentren befinden sich in der Schweiz und sind örtlich voneinander getrennt.

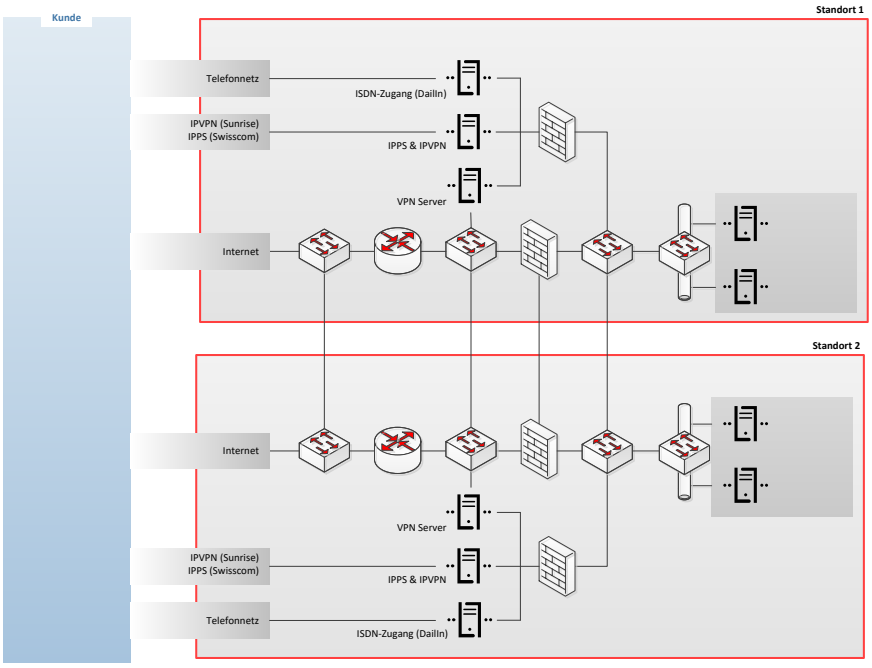


**Abbildung 1 Systemarchitektur**

Alle Leitungen bei Dolphin Systems sind so geführt, dass immer eine Redundanz vorhanden ist. Telefonleitungen und Internetanbindung sind doppelt und soweit technisch möglich über unterschiedliche Provider angebunden. Die beiden Standorte sind über einen Glasfaserring verbunden, was eine ausgezeichnete Verfügbarkeit mit schneller Fehlererkennung koppelt.

### *3.1.2 Rechenzentren*

Die Rechenzentren erfüllen die strengen Vorgaben der internationalen Norm ISO/IEC 27001, eine neutrale Instanz zur Informationssicherheit. Die Prüfung beinhaltet die Kontrolle von Einführung, Betrieb und Überwachung eines dokumentierten Informationssicherheits-Managementsystems für das jeweilige Unternehmen unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.

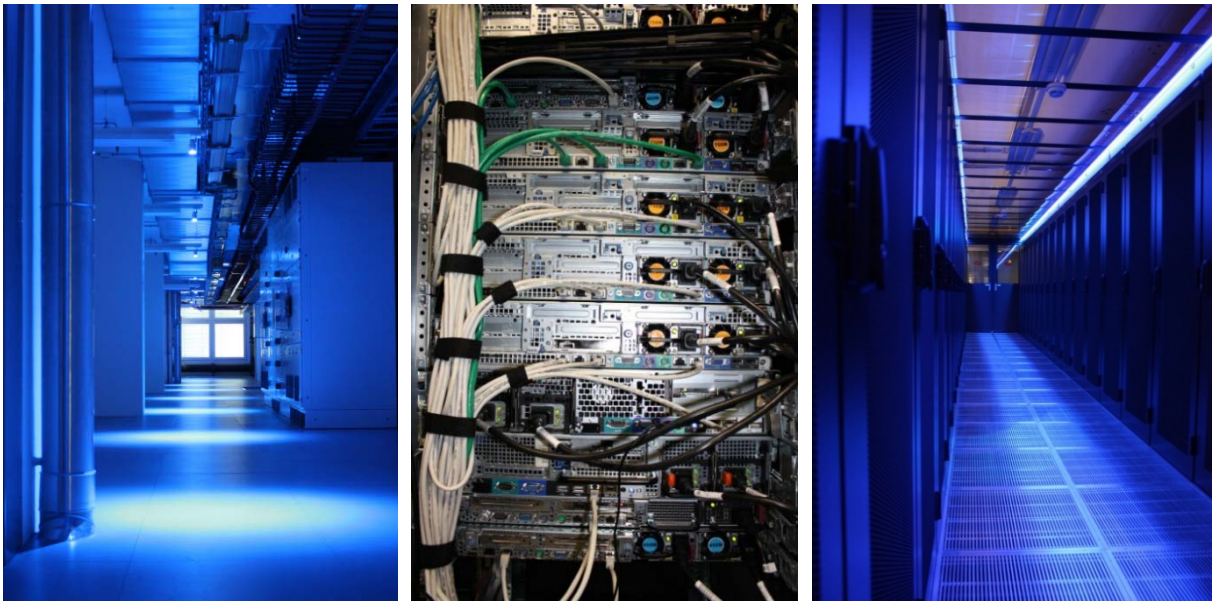

**Abbildung 2 Rechenzentren**

Die Rechenzentren bieten uns unterbrechungsfreie Stromversorgung (USV) und eine Redundanz von N+1 bei einer nachgewiesenen Verfügbarkeit von 99,999 Prozent. Des Weiteren eine hohe Widerstands-fähigkeit dank eines robusten HVAC-Systems und leistungsfähige Kühlsysteme, die Einhaltung strengster Sicherheitsvorgaben und ein Höchstmass an operativer Zuverlässigkeit und leistungsstarke und gesicherte Anbindung dank einer Glasfaserringverbindung. Die Leitungen sind in verschlossenen und gesicherten Räumlichkeiten geführt. Drahtlose Netzwerke wie Wireless LAN sind innerhalb der Systemumgebung nicht gestattet. Die Server sind dank einer 24-Stunden-Zugangskontrolle vor unerlaubtem Zutritt geschützt. Sicherheitspersonal, Schliess- und Überwachungssysteme, Überwachungskameras, Anwesenheits- und Wassersensoren sowie Löschvorrichtungen sorgen zusätzlich für die nötige Sicherheit.

### *3.1.3 Überwachungssysteme*

Sämtliche im Einsatz stehende Systeme sind 7 x 24h überwacht und melden Fehlverhalten, Störungen und Ausfälle automatisch den zuständigen Technikern. Die Überwachung aller Systeme bedingt die Kontrolle sowohl interner als auch externer Systeme. Für das Sicherstellen dieser Überwachung setzen wir auf verschiedene professionelle Instrumente, welche regelmässige

Kontrollen und Messungen durchführen. Ein Problem oder gar ein Ausfall eines Systems wird sofort angezeigt und es kann schnell mit der Problembehebung begonnen werden. Die dazugehörende Software erlaubt einen guten Überblick über sämtliche Systeme, welche in Betrieb sind. Es lässt aber auch detaillierte Messungen jedes einzelnen Systems zu.

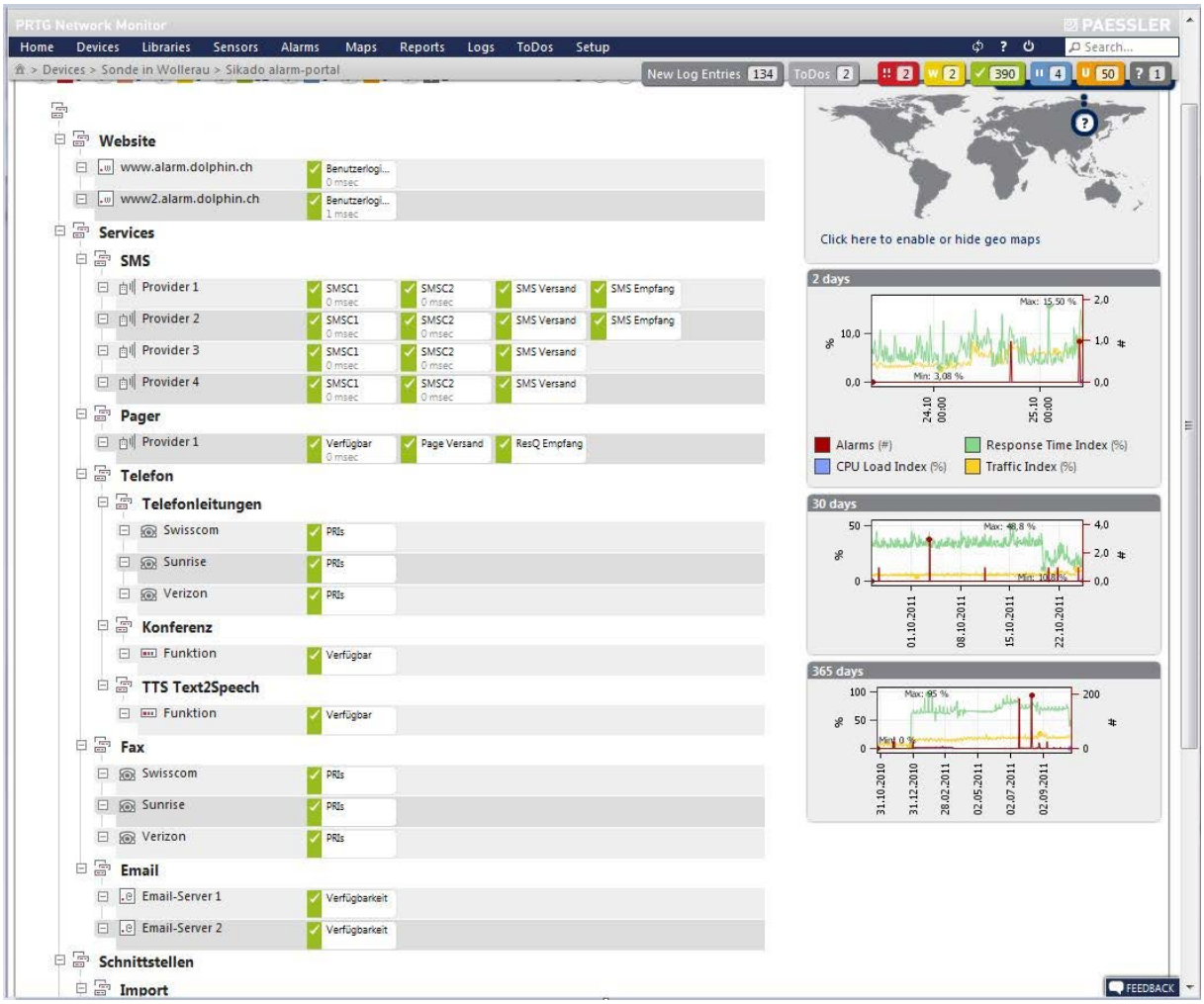


Abbildung 3 **Überwachungssystem** bei Dolphin Systems

### *3.1.4 Bereichsabhängige Zugriffsrechte*

Unterschiedliche Zugriffsrechte für verschiedene Bereiche gewährleisten einerseits jederzeit auf die Systeme zuzugreifen, andererseits bieten sie Schutz vor unerlaubten Zugriffen. Das Prinzip hinter dieser Strategie ist, für jeden Bereich den Zugang nur soweit wie nötig zu erlauben. Besonders kritische Bereiche und Systeme sind von aussen nicht erreichbar, andere wiederum nur über VPN mit stark eingeschränkten Rechten. Sämtliche Systeme sind auf mehreren Ebenen passwortgeschützt. Passwörter sind verschlüsselt und nicht im Klartext abgelegt.

### *3.1.5 Updates, Systemerneuerungen und Firewalls*

Werden für die bei uns zum Einsatz kommenden Programme und Software Aktualisierungen angeboten, führen wir die nötigen Updates durch, denn diese bieten nicht nur Erweiterungen und eine verbesserte Funktionalität, sondern beheben häufig auch Sicherheitslücken. Ähnliches gilt für Hardware- Komponenten: Gibt es technische Neuerungen, welche die Sicherheit und Zuverlässigkeit der Systeme deutlich erhöhen, werden die Teile ersetzt. Somit sind Software und System immer auf dem aktuellen Stand der Technik. Regelmässige Aktualisierungen werden vor allem auch bei Antivirenprogrammen durchgeführt. Gegen unerwünschte Zugriffe von aussen ist eine restriktive Firewall installiert.

### *3.1.6 Sicherungskopien*

Von allen wichtigen Dateien und Datenbanken wird täglich eine Sicherungskopie erstellt, so dass im Falle eines Verlusts oder Beschädigung des Originals keine Informationen verloren gehen. Eine solche Sicherungskopie gewährleistet zudem jederzeit über die Daten zu verfügen. Die Backup-Software erledigt diese Aufgabe automatisch und zuverlässig.

### *3.1.7 Protokollierung - Aufzeichnung*

Automatisch erstellte Protokolle und Logdateien helfen, zu einem späteren Zeitpunkt zu ermitteln, wie es zu Fehlern oder Schäden bei einem Rechnersystem oder Software gekommen ist. Dafür werden sämtliche Aktionen, Änderungen und Abläufe systematisch aufgezeichnet und festgehalten. Auch die Bedienung der Systeme von den Benutzern und Anwendern wird protokolliert. Bei Bedarf können die gesammelten Informationen ausgewertet werden. Damit lassen sich schnell konkrete Rückschlüsse auf mögliche Ursachen machen. Allfällige Anpassungen und Fehlerbehebungen können somit effizienter umgesetzt und behoben werden.

## 3.2 Organisatorische Massnahmen

Neben den technischen Massnahmen für die Datensicherheit sind die organisatorischen ebenfalls von grosser Wichtigkeit. Denn viele technische Massnahmen nützen nichts oder nur wenig, wenn sie aufgrund schlechter oder unzureichender Organisation umgangen, missachtet oder als unwichtig betrachtet werden. In den meisten Fällen, wo die Datensicherheit gefährdet oder nicht gewährleistet wurde, geschah dies aus Unwissenheit, Unaufmerksamkeit, unklaren Zuständigkeiten und organisatorischen Unklarheiten. Wir sind davon überzeugt, dass durch klare Strukturen, kompetente Mitarbeitende, sinnvolle Richtlinien und konsequentes, richtiges Verhalten ein hohes Mass an Datensicherheit gewährleistet werden kann.

### 3.2.1 Klare Strukturen und Verantwortung

Betriebliche Prozesse werden nach sicherheitsrelevanten Aspekten durchleuchtet und entsprechend angepasst. Für sämtliche Arbeiten und Projekte müssen die Ziele der Datensicherheit eingehalten werden. Es gehört zu der Verantwortung jedes einzelnen Mitarbeitenden, sich an die Richtlinien und Weisungen über die Datensicherheit zu halten. Deshalb wird bei Stellenantritt jedes Mitarbeitenden auf die gültigen Richtlinien hingewiesen. Bei Arbeiten, welche die Datensicherheit tangieren, müssen die verantwortlichen Vorgesetzten informiert werden. Stellt ein Mitarbeitender eine Unregelmässigkeit fest oder vermutet Lücken im Sicherheitskonzept, informiert er seinen Vorgesetzten, damit dieser die nötigen Massnahmen ergreifen kann.

### 3.2.2 Schulung der Mitarbeitenden

Dolphin Systems schult ihre Mitarbeitenden regelmässig. Ziel dabei ist, einerseits ein Bewusstsein für den sicheren Umgang mit Daten zu schaffen, andererseits die Mitarbeitenden dazu zu befähigen, gewissenhaft und sorgfältig zu arbeiten. Daneben werden die internen Richtlinien betreffend Datensicherheit vermittelt und die neuesten Erkenntnisse und Erfahrungen ausgetauscht. Wir sind davon überzeugt, dass geschulte und kompetente Mitarbeitende einen wesentlichen Beitrag zur Datensicherheit leisten können.

### 3.2.3 Verhalten bei Fehlfunktionen

Meldet das Überwachungssystem eine Fehlfunktion oder gar einen Ausfall, wird automatisch ein Techniker informiert. Mittels Remote-Zugriff kann dieser auf das defekte System zugreifen und die nötigen Massnahmen einleiten. Diese erlaubt uns, die meisten Fehlfunktionen und Ausfälle mit sehr kurzen Reaktionszeiten zu beheben. Zur gleichen Zeit wird auf das redundante System umgeschaltet, welches sofort sämtliche Funktionen übernimmt. Somit ist die Verfügbarkeit der Systeme fast ausnahmslos gewährleistet. Der Kunde wird über Fehlfunktionen oder Ausfälle normalerweise per E-Mail informiert. In dringenden Fällen kann dies auch per SMS oder Anruf geschehen.

### *3.2.4 Richtlinien*

Als Instrument der internen Sicherheitsstrategie werden Richtlinien festgelegt, welche im Rahmen der internen Schulung den Mitarbeitenden vorgelegt werden. Diese Richtlinien dienen als Leitfaden für die täglichen Arbeiten bei Dolphin Systems und regeln die konkrete Umsetzung der Ziele im Bereich der Datensicherheit.

### *3.2.5 Auditing*

Um die Erbringung der Datensicherheit zu gewährleisten, ist eine regelmässige Überprüfung Pflicht. Dolphin Systems wurde in der Vergangenheit von verschiedenen namhaften Unternehmen auditiert und als Serviceanbieter von diesen zugelassen.

# 4. Zusammenfassung

In unserer vernetzten Welt bedarf das Thema Datenschutz und Datensicherheit grösster Sorgfalt. Der Begriff Datensicherheit ist bevorzugt zu verwenden und bezieht den Datenschutz als Teil dessen mit ein. Datensicherheit deckt die drei Ziele: Einhaltung der gesetzlichen Bestimmungen, Erfüllung der Unternehmensphilosophie und Gewährleistung der Informationssicherheit. Für die Umsetzung dieser Ziele setzt Dolphin Systems ein Bündel an technischen und organisatorischen Massnahmen ein.

Die Systemarchitektur ist so aufgebaut, dass es für jedes System ein redundantes Ersatzsystem gibt, welches bei Störungen und Ausfällen zur Verfügung steht und die nötige Verfügbarkeit garantiert. Die Rechenzentren, welche die strengen Vorgaben der internationalen Norm ISO/IEC 27001 erfüllen, bieten uns eine zuverlässige, leistungsstarke und sichere Plattform für unsere Dienstleistungen und Services. Überwachungssysteme kontrollieren sämtliche Systeme 7 x 24h und melden Fehlverhalten, Störungen und Ausfälle automatisch den zuständigen Technikern.

Unterschiedliche Zugriffsrechte für verschiedene Bereiche gewährleisten einerseits, jederzeit auf die Systeme zugreifen zu können, andererseits bieten sie Schutz vor unerlaubtem Zugriff. Software-Aktualisierungen vor allem auch bei Antivirenprogrammen verbessern nicht nur die Funktionalität, sondern beheben auch Sicherheitslücken. Gegen unerwünschte Zugriffe von aussen sind restriktive Firewalls installiert. Von sämtlichen Dateien wird täglich eine Sicherungskopie erstellt, so dass im Falle eines Verlusts des Originals keine Informationen verloren gehen. Automatisch erstellte Protokolle und Logdateien helfen, zu einem späteren Zeitpunkt zu ermitteln, wie es zu Fehlern oder Schäden bei einem Rechnersystem gekommen ist. Sämtliche Aktionen, Änderungen und Abläufe werden systematisch aufgezeichnet und können bei Bedarf ausgewertet werden, um konkrete Rückschlüsse auf mögliche Ursachen von Fehlern zu machen.

Neben den technischen Massnahmen für die Datensicherheit sind die organisatorischen ebenfalls von grosser Wichtigkeit. Nur durch klare Strukturen, kompetente Mitarbeitende, sinnvolle Richtlinien und konsequentes, richtiges Verhalten kann ein hohes Mass an Datensicherheit erreicht werden. Dolphin Systems setzt auf klare Strukturen und Verantwortung im Umgang mit Daten. Ziel bei der Schulung der Mitarbeitenden ist einerseits, das Bewusstsein für den sicheren Umgang mit Daten zu schaffen, andererseits die Mitarbeitenden zu befähigen, gewissenhaft und sorgfältig zu arbeiten. Daneben werden die internen Richtlinien betreffend Datensicherheit vermittelt und die neuesten Erkenntnisse und Erfahrungen ausgetauscht. Wir sind davon überzeugt, dass geschulte und kompetente Mitarbeitende entscheidend zur Erbringung der Datensicherheit beitragen können.
Um die Erbringung der Datensicherheit zu gewährleisten, ist eine regelmässige Überprüfung Pflicht. Dolphin Systems wurde in der Vergangenheit von verschiedenen namhaften Unternehmen auditiert und als Serviceanbieter von diesen zugelassen.