ENABLING PEOPLE
IMPROVING BUSINESS

Datenschutzkonzept

PROVECTUS SOFTWARE GMBH

Informationsersteller:	Geschäftsführung
Empfänger / Verteilerkreis:	keine Einschränkungen
Einschränkungen:	keine Einschränkungen

Inhalt

1. Sicherheitsleitlinie

1.1 SICHERHEITSPOLITIK

Informationsverarbeitung und der Schutz personenbezogener Daten sind in unserem Unternehmen von höchster Bedeutung. Geschäftsprozesse und die Erfüllung unserer Aufgaben werden maßgeblich durch den Einsatz von Informationstechnik ermöglicht. Störungen und Ausfälle müssen daher vermieden und notfalls kurzfristig kompensiert werden.

Das Thema Informationssicherheit umfasst sämtliche technischen, personellen und organisatorischen Maßnahmen, um erforderliche Sicherheit hinsichtlich Verfügbarkeit, Integrität und Vertraulichkeit zu gewährleisten. Informationssicherheit betrifft nicht nur technisch versiertes IT-Personal, sondern jeden, der mit Informationen umgeht. Jeder Mitarbeiter muss sich der Notwendigkeit der Informationssicherheit bewusst sein und entsprechend handeln.

Aufgrund der starken Abhängigkeit nahezu all unserer Unternehmensprozesse von der Informationstechnik ist die Informationssicherheit somit ein integraler Bestandteil unserer Unternehmensstrategie. Darüber hinaus werden gesetzliche Regelungen und Vorschriften, z.B. zum Datenschutz erfüllt.

1.2 ZIELE

Ziel dieser Sicherheitspolitik ist die Richtungsvorgabe und Unterstützung der Geschäftsführung bei der Informationssicherheit in Übereinstimmung mit Geschäftsanforderungen, sowie geltenden Gesetzen und Regelungen.

Unser oberstes Ziel ist es, die Verfügbarkeit, Vertraulichkeit und Integrität der eigenen und der uns von Kunden und externen Partnern anvertrauten Informationen und Ressourcen zu schützen.

Die Nachvollziehbarkeit, Verbindlichkeit und Ordnungsmäßigkeit von Prozessen wird dabei garantiert, um das Erreichen der Unternehmensziele zu gewährleisten und Schaden zu verhindern oder zu begrenzen. IT-unterstützte Prozesse sind immer dem Spannungsfeld zwischen Sicherheit, Handlungsfähigkeit und Wirtschaftlichkeit ausgesetzt.

Jede Maßnahme zur Erhöhung der Informationssicherheit darf die Handlungsfähigkeit nicht unangemessen beeinträchtigen und muss im Gesamtzusammenhang wirtschaftlich sein. Der Schutz von Informationen und Ressourcen dient auch der Rechtssicherheit der Mitarbeiter, Kunden und externen Partner.

Die Informationssicherheit der Provectus Software GmbH basiert auf folgenden Detailzielen:

- **Informationssicherheit ist eine Leitungsaufgabe und geht von der Geschäftsführung aus**. Die Durchsetzung, Aufrechterhaltung und dauerhafte Fortentwicklung des Informationssicherheitsmanagementsystems (ISMS) wird durch die Tatsache gewährleistet, dass die Geschäftsführung das System initiiert hat und fortlaufend aktiv unterstützt.

- **Gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen werden erfüllt**.
- Eine absolute Sicherheit der Informationssicherheits-Infrastruktur ist nicht realisierbar. Viele Beeinträchtigungen der Informationssicherheit beruhen jedoch auf allgemein bekannten Schwachstellen, die bei **sachgemäßer Handhabung und Organisation** zu beherrschen sind. Hierfür haben wir Konzepte und Prozesse definiert, die in unseren technisch-organisatorischen Maßnahmen dargestellt sind.
- Die **Verarbeitung firmeneigener personenbezogener Daten** im Sinne des Datenschutzgesetzes wird auf das **notwendige Maß reduziert bzw. vermieden**.
- Ein qualifizierter Sicherheitsstandard wird mit **zusätzlichem personellem, zeitlichem und finanziellem Aufwand** hergestellt und aufrechterhalten. Qualifizierte Mitarbeiter mit hohem Expertenwissen und detaillierten Kenntnissen der Informationssicherheits-Infrastruktur und diesbezüglichen Prozessen werden im Unternehmen eingesetzt, um detaillierte Risikoanalysen zur Erkennung und Abwehr von Sicherheitslücken durchzuführen. Verantwortlichkeiten sind definiert, eine Aufgaben- und Funktionstrennung wird durchgeführt, sowie Zutritts- und Zugriffsrechte aufrechterhalten. Wartungs- und Entsorgungsaufgaben sind ebenfalls geregelt.
- Laufend verbesserte Informationssicherheit wird erreicht, indem **unternehmensweit gültige Standards** definiert und diese unternehmensweit ggf. gestuft auf den Ebenen von Arbeitsgruppen, Abteilungen und externen Partners erfolgreich umgesetzt werden.
- **Informationssicherheit ist eine Gemeinschaftsaufgabe**, die von allen Beschäftigten wahrgenommen werden muss. Eine erfolgreiche Umsetzung wird dadurch ermöglicht, dass die Beschäftigten von Beginn an für die Belange der Informationssicherheit sensibilisiert, in den Prozessen geschult und das Gefährdungspotential und mögliche Gegenmaßnahmen in ihrem Arbeitsumfeld informiert werden. Anlaufpunkte und Verantwortliche zur Entgegennahme zur Meldung von Sicherheitsverstößen sind eingerichtet.
- Auf Daten und Anwendungen dürfen grundsätzlich nur Personen zugreifen, die eine entsprechende Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt der Geschäftsführung. Zur Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten wird die/der Datenschutzbeauftragte rechtzeitig eingebunden. Gleiches gilt für die Neueinführung und Änderung der entsprechenden Verfahren. Vertrauliche Informationen sind stets vor unbefugten Zugriff zu schützen. (**Vertraulichkeit**).
- Daten und Anwendungen sind, dem jeweiligen Nutzungsprofil und zeitlichen Anforderungsprofil entsprechend, vom Arbeitsplatz aus bei Bedarf verfügbar. Für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung / Archivierung der IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle und deren Wiederherstellbarkeit – auch bei Notfällen – in einem festgelegten Zeitrahmen und Umfang geregelt (**Verfügbarkeit**).
- Daten und Anwendungen dürfen nicht unberechtigt gelöscht / zerstört oder manipuliert werden können (**Integrität**). Verschlüsselungs- und Virenschutzsysteme schützen die Integrität.
- Es ist sichergestellt, dass Maßnahmen, die die Informationssicherheit beeinträchtigen, dokumentiert werden.
- Die Sicherheitsstandards werden permanent weiterentwickelt, so dass zeitnah neue Risiken erkannt und geeignete Gegenmaßnahmen ergriffen werden können.

Alle Angehörigen des Unternehmens beachten Gesetz und vertragliche Vereinbarungen. Die Geschäftsführung ist sich seiner Verantwortung zur Informationssicherheit bewusst, steuert die Prozesse im Unternehmen dementsprechend und stellt angemessene Ressourcen zur Erreichung der Ziele bereit. In manchen Fällen werden durch unser Unternehmen auch Informationen zu fremden Zwecken verarbeitet, die durch Gesetze und aufgrund von Verträgen sorgfältig und vertraulich zu behandeln sind. Hierzu werden angemessene Vorkehrungen getroffen, welche im weiteren Verlauf dieses Konzeptes konkretisiert werden.
Zur Vermeidung von Vorfällen und Schäden in allen genannten Bereichen werden möglichst wenige Informationen erhoben und genutzt. Die Grundsätze der Datenvermeidung und der Datensparsamkeit werden damit selbstverständlich beachtet.
Elektronische Kommunikation ist für unsere tägliche Arbeit und die von uns angebotenen Leistungen unabdingbar und der Einsatz des Internets selbstverständlich. Durch angemessene Maßnahmen im Rahmen dieses Konzepts sind die hiermit verbundenen Risiken möglichst reduziert.

1.3 ORGANISATION

Zur Erfüllung und Überwachung sämtlicher Daten- und Informationssicherheitsvorgaben wurde in unserem Unternehmen eine geeignete Sicherheitsorganisation geschaffen und Verantwortliche benannt:

- **Informationssicherheitsbeauftragter**
  Es ist ein Informationssicherheitsbeauftragter bestellt. Dieser ist direkt verantwortlich für die Ausgestaltung der Informationssicherheit gemäß der von der Geschäftsführung vorgegebenen Sicherheitspolitik und berichtet in seinem Aufgabenbereich.
- **Datenschutzbeauftragter**
  Es ist ein Datenschutzbeauftragter bestellt, der im Rahmen seiner gesetzlichen Aufgaben das Unternehmen, alle Beschäftigten und Betroffene in Angelegenheiten des Datenschutzes unterstützt.

Mitarbeiter beachten die Anweisungen des Informationssicherheitsbeauftragten oder des von ihm beauftragten Personals in sicherheitsrelevanten Angelegenheiten.
In Angelegenheiten des Datenschutzes können Mitarbeiter, externe Partner und Kunden sich direkt an den Datenschutzbeauftragten wenden.
Alle Mitarbeiter unterstützen die Beauftragten angemessen in ihrer Arbeit. Die Beauftragten werden frühzeitig in für ihren Aufgabenbereich relevante Planungen einbezogen. Mitarbeiter sind angemessen auf ihre Aufgaben vorbereitet und bezüglich der Anforderungen geschult.

1.3.1 KONTAKT DATENSCHUTZBEAUFTRAGTER

Firma: activeMind AG Management- und Technologieberatung
Name: Herr Valentin Wingerter
E-Mail: wingerter@activemind.legal
Tel.: +49 (0)89 / 919294900

1.3.2 KONTAKT INFORMATIONSSICHERHEITSBEAUFTRAGTER

Firma: activeMind AG Management- und Technologieberatung
Name: Jan Baumgärtner
E-Mail: baumgaertner@activemind.de
Tel.: +49 (0)30 / 770191070

1.4 ORGANISATION

In unserem Unternehmen sind gesteuerte Prozesse geregelt und dokumentiert. Diese sind messbar, werden regelmäßig überprüft und nach Bedarf korrigiert.
Es bestehen unter anderem folgende Informationssicherheits-, Datenschutzregelungen und Prozesse im Unternehmen:

1.4.1 LEITLINIEN, KONZEPTE UND REGELUNGEN

- Sicherheitsleitlinie (Teil dieses Dokuments)
- Informationssicherheitshandbuch (ISMS Handbuch)
- 06_Konzept_Informationssicherheitsorganisation
- 07_Konzept_Personalsicherheit
- 08_Konzept_Verwaltung der Werte
- 09_Konzept_Zugangssteuerung
- 10_Konzept_Kryptographie
- 11_Konzept_Physische und umgebungsbezogene Sicherheit
- 12_Konzept_Betriebssicherheit
- 13_Konzept_Kommunikationssicherheit
- 14_Konzept_Anschaffung, Entwicklung und Instandhaltung von Systemen
- 15_Konzept_Liefrantenbeziehungen
- 16_Konzept_Management von Informationssicherheitsvorfällen
- 17_Konzept_Informationssicherheitsaspekte beim Business Continuity Management
- 18_Konzept_Complinace
- Richtlinie Klassifizierung von Informationen und deren Umgang im Unternehmen
- IT-Nutzungsrichtlinie (inkl. Regelungen für Mobilgeräte und Telearbeit)
- Clean Desktop Regelung
- Regelungen zur Einschränkung von Softwareinstallationen
- Regelungen zur Datensicherung
- Regelungen für den Schutz vor Schadsoftware
- Regelungen für die Handhabung technischer Schwachstellen
- Regelungen zur Löschung von Daten

1.4.2 ITIL PROZESSE

- Prozess Incidentmanagement
- Prozess Problemmanagement
- Prozess Changemanagement

1.4.3 ITIL WARENWIRTSCHAFTSPROZESSE

- Prozess Wareneingang / Warenausgang
- Prozess Auftragsprüfung und Einkauf
- Prozess Angebotserstellung
- Prozess Auftragsabwicklung
- Prozess internes Audit

2. Technische und organisatorische Maßnahmen

Dieses Kapitel beschreibt alle technischen und organisatorischen Maßnahmen, welche zur Gewährleistung von Datenschutz und Informationssicherheit festgelegt wurden. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Unternehmen verarbeiteten Informationen und Daten.

2.1 SICHERHEITSLEITLINIE

Die in diesem Datenschutzkonzept zu Beginn aufgeführte Sicherheitsrichtlinie beinhaltet die Leitaussagen der Geschäftsführung zur Informationssicherheit in unserem Unternehmen. Alle Beschäftigten, freien Mitarbeiter und externe Partner werden im Rahmen ihrer jeweiligen vertraglichen Vereinbarungen auf unsere Informationssicherheitsgrundsätze und den Datenschutz verpflichtet.

Das erreichte Informationssicherheitsniveau wird durch eine Kombination aus periodisch wiederkehrenden Prüfungen und kontinuierlichen Kontrollen überwacht.
Die Überwachung des laufenden Betriebs erfolgt in Abstimmung mit dem Informationssicherheitsbeauftragten.

Ein Review der Sicherheitspolitik erfolgt zumindest jährlich, soweit nicht eine essentielle Änderung dies früher erfordert. Hierdurch wird die laufende Angemessenheit, Eignung und Effektivität der Regelung sichergestellt.

Die Geschäftsführung ist für die Informationssicherheitspolitik zuständig und hat die Verantwortung, diese zu entwickeln, zu überarbeiten und zu prüfen.

2.2 ORGANISATION DER INFORMATIONSSICHERHEIT

Die Geschäftsführung der Provectus Software GmbH ist für die vollständige Umsetzung der in der Sicherheitsrichtlinie dargelegten Ziele der Informationssicherheit und für die Erfüllung der an sie gestellten Informationssicherheitsaufgaben verantwortlich.

Informationssicherheitsrollen und -verantwortlichkeiten sind in unserem Konzept „IT Sicherheitsorganisation“ definiert und beschrieben. Aus diesem ergibt sich die Zuständigkeit der Verantwortlichen für die Aufgaben im Rahmen der Informationssicherheit; u.a. sind dort auch das Informationssicherheitsteam und das Interventionsteam festgelegt.

Wir verfügen über ein Verfahren, das festlegt, wann und durch wen relevante Behörden benachrichtigt und erkannte Datenschutz- und Informationssicherheitsvorfälle rechtzeitig gemeldet werden.
Auch pflegen wir laufenden Kontakt zu speziellen Interessensgruppen (z.B.: Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.), um über Änderungen und Verbesserungen im Bereich Datenschutz und Informationssicherheit informiert zu sein.

Unserer Projektmethodik sieht vor, dass Datenschutz und Informationssicherheit fester Bestandteil aller Projektphasen ist.

Durch unsere jeweiligen Richtlinien und Prozesse stellen wir den Datenschutz und die Informationssicherheit auch in allen Bereichen unseres eigenen Unternehmens sicher.

2.3 PERSONALSICHERHEIT

Im Rahmen unseres Einstellungsprozesses wählen wir unsere Beschäftigten sorgsam aus und prüfen ihre Eignung für ihre vorgesehene Position und Rolle im Unternehmen. Ihre Verantwortlichkeiten haben wir in Stellen- und Rollenbeschreibungen festgelegt und gleichen regelmäßig in Mitarbeitergesprächen ab, ob Sie diesen entsprechen. Vor Beginn ihrer Anstellung unterschreiben alle Beschäftigten eine Vertraulichkeits- sowie Datenschutzvereinbarung, die über die Beendigung des Beschäftigungsverhältnisses hinaus gilt.

Die Beschäftigten werden im Bereich Datenschutz- und Datensicherheit regelmäßig geschult, insbesondere werden Schulungen bei einem Positionswechsel noch einmal aufgefrischt. Sie sind sich daher ihrer Verantwortung diesbezüglich bewusst.

In unserem Personalkonzept dokumentieren wir den Prozess für die Zeit vor, während und nach Beendigung des Beschäftigungsverhältnisses, und stellen sicher, dass personenbezogene Daten geschützt und die Informationssicherheit gewährleistet ist. Diese beinhaltet auch Maßregelungen für den Fall eines Datenschutzverstoßes.

2.4 VERWALTUNG DER WERTE

Sämtliche Werte (wie z.B. Betriebsmittel, Wechseldatenträger, Laptops) und Informationen, die mit personenbezogenen Daten in Zusammenhang stehen, werden von uns inventarisiert und gepflegt. Zum Schutz dieser Werte haben wir Verantwortliche festgelegt, die für den Lebenszyklus eines Wertes

zuständig sind. Es wurden dokumentierte Regeln für den zulässigen Gebrauch unserer Werte aufgestellt und allen Beschäftigen mitgeteilt. Die Rückgabe von Werten erfolgt dokumentiert.

Unsere Informationen und Daten werden anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert und gekennzeichnet. Diesem Klassifizierungsschema entsprechend, haben wir dokumentierte Verfahren für die Handhabung unserer Werte, insbesondere auch unserer Wechseldatenträger, entwickelt und umgesetzt.

In unserem Konzept zur Verwaltung von Betriebsmitteln definieren wir einen dokumentierten und geregelten Prozess zum Transport von Datenträgern, um diese vor unbefugtem Zugriff, Missbrauch oder Verfälschung zu schützen. Nicht mehr benötigte Datenträger entsorgen wir sicher und unter Anwendung formaler Verfahren.

2.5 ZUGRIFFSSTEUERUNG

Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogenen Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Es ist sichergestellt, dass ausschließlich befugte Benutzer Zugang zu Systemen, Netzwerken und Diensten haben und unbefugter Zugang unterbunden wird. Insbesondere besteht ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern, der die Zuordnung von Zugangsrechten ermöglicht.

Berechtigungen zum Zugriff auf IT-Systeme werden über ein geregeltes Verfahren auf der Grundlage eines dokumentierten und restriktiven Berechtigungskonzepts vergeben. Ist- und Soll-Zustand von Benutzerzugangsrechten werden regelmäßig abgeglichen und bei Bedarf entzogen oder angepasst.
Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Hierzu verwenden wir ein System zur Nutzung sicherer und starker Kennwörter, welche einem geregelten und dokumentierten Prozess unterliegen.

Unsere administrativen Rechte erteilen wir eingeschränkt und gesteuert.
Der Gebrauch von Hilfsprogrammen, die fähig sein könnten, System- und Anwendungsschutzmaßnahmen zu umgehen, ist eingeschränkt und streng überwacht.
Der Zugang zu Quellcodes von Programmen ist eingeschränkt.

2.6 KRYPTOGRAPHIE

Der angemessene und wirksame Gebrauch von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information ist sichergestellt. Zu diesem Zwecke haben wir eine Richtlinie über den Einsatz von Kryptographischen Maßnahmen im Unternehmen implementiert, die auch die Verwaltung von kryptographischen Schlüsseln umfasst und dem Schutzbedarf angemessen ist.

2.7 PHYSISCHE UND UMGEBUNGSBEZOGENE SICHERHEIT

In unserem Konzept zum Schutz vor physischem Zugang und Umwelteinflüssen haben wir dokumentierte und geregelte Maßnahmen getroffen, die verhindern sollen, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Zu diesem Zweck lagern wir sämtliche Datenverarbeitungssysteme in ein externes und stark abgesichertes Rechenzentrum aus und betreiben an unserem Geschäftsstandort ausschließlich die notwendige Zugriffs- und Netzwerkinfrastruktur, um über das Internet auf diese Systeme zugreifen zu können.

2.7.1 GESCHÄFTSSTANDORT „PROVECTUS GMBH, LEOPOLDSTR. 250B, 80807 MÜNCHEN“

- Die Geschäftsräume liegen im Erdgeschoß eines Bürogebäudes und werden exklusiv genutzt.
- Es existiert nur ein zentraler Eingang.
- Außentüren und Türen zu Sicherheitsbereichen sind geschlossen.
- Der Zugang zu den Geschäftsräumen und Sicherheitsbereichen erfolgt durch eine elektronische Schließanlage mit Kartenlesegeräten. Zutritte werden erfasst und können im Schadfall durch einen geregelten Prozess analysiert werden.
- Besucher oder externe Dienstleister werden individuell eingelassen.
- Für kritische Sicherheitsbereiche ist eine Alarmanlage vorhanden und außerhalb der Geschäftszeiten aktiv.
- Der Brandschutz wird beachtet.
- Es sind Sicherheitsbereiche vorhanden, zu denen nur eigens hierzu Berechtigte Zutritt erhalten.
- IT-Räume und Serverschränke sind separat verschlossen und nur durch Berechtigte zu öffnen.
- Die Sicherheit der Verkabelung wird beachtet.
- Die Instandhaltung von Systemen wird geplant oder umgesetzt.
- Das Entfernen von Systemen und Informationen erfolgt geregelt.
- Die Sicherheit von Systemen außerhalb der Räumlichkeiten wird beachtet.
- Die Entsorgung oder Wiederverwendung von Betriebsmitteln erfolgt geregelt.
- Unbeaufsichtigte Benutzergeräte werden geschützt, u.a. sind die Benutzer angehalten, sich aus nicht mehr benötigten Netzwerkdiensten abzumelden und nicht genutzte Geräte entsprechend zu sperren
- Richtlinien für Clean Desk und Bildschirmsperren werden umgesetzt.

2.7.2 RECHENZENTRUMSSTANDORT „NORIS NETWORK AG, KLAUSNERSTRAßE 30, 85609 ASCHHEIM“

Die physische und umgebungsbezogene Sicherheit stellen wir durch entsprechende Service Level Agreements und diesbezügliche regelmäßige Kontrollen (auch in unserem externen Rechenzentrum)

sicher. Wir haben das Rechenzentrum der noris network AG vor dem Vertragsabschluss sorgfältig geprüft und einen AV-Vertrag abgeschlossen.

Für die physische und umgebungsbezogene Sicherheit werden von der noris network AG folgende Maßnahmen getroffen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile.
- Die Rechenzentren haben keine Fenster; Türen schließen selbsttätig.
- Die Türzutrittskontrollprotokolle werden gesichtet, stichprobenartig überprüft und archiviert.
- Zutrittskontrollsysteme an den Eingängen zu Büroräumlichkeiten.
- Beschäftigte sind angewiesen, Fenster und Türen außerhalb der Bürozeiten geschlossen bzw. verschlossen zu halten.
- Ein Sicherheitsdienst überprüft außerhalb der Bürozeiten, dass Fenster und Türen geschlossen sind.
- Eine Gefahrenmeldeanlage für Brand- und Alarmdetektion ist durchgängig über das noris-network-Monitoring realisiert.
- Ein Notfallplan besteht.
- Die Rechenzentren sind jeweils in der Schleuse und in den Rechenzentren videoüberwacht.
- Stichproben der digitalisierten Bewegungsbilder im Rechenzentrum werden durchgeführt und mit den archivierten Daten (Zutrittskontrollprotokolle) abgeglichen.
- Geregelte Prozesse für die Schlüsselverwaltung / Ausweisverwaltung sind vorhanden, die Zuständigkeit hierfür liegt bei der Personalverwaltung.
- Der Zutritt von Fremdpersonen, z.B. externe Dienstleister, ist geregelt und unterliegt entsprechenden Schutzbestimmungen von noris network AG (spezielle Prozessdefinitionen beim Zutritt zum Rechenzentrum: Umfang, Zeitpunkt, Firmenname, Name mit Unterschrift, spezifische Zutrittskontrollkarte, Begleitung eines Beschäftigten, Kameraüberwachung etc.). Diese werden dokumentiert und protokolliert.
- Der Zutritt zum Rechenzentrumsbereich während und außerhalb der Geschäftszeiten ist geregelt und protokolliert.
- In den Rechenzentren finden regelmäßige Kontrollgänge statt.
- Der Umgang mit und die Sicherheit von mobilen Datenträgern ist geregelt.
- Das Rechenzentrum ist in getrennte Schutzzonen aufgebaut, für die der Zutritt geregelt ist.
- Notausgänge sind alarmgesichert.
- Zusätzliche, umfangreiche Zertifizierungen (u.a. das ISO/IEC 27001 auf Basis des IT-Grundschutzes des BSI)

2.8 BETRIEBSSICHERHEIT

In unserem Konzept zur Betriebssicherheit definieren wir geregelte und dokumentierte Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb von informations- und datenverarbeitenden Einrichtungen sicherzustellen. Diese umfassen sowohl die Steuerung im Falle einer Änderung an den

informationsverarbeitenden Einrichtungen, als auch eine Steuerung und regelmäßige Messung unserer Kapazitäten und Ressourcen, um die Verfügbarkeit der erforderlichen Systemleistung sicherzustellen.
In unserem Unternehmen ist es essentiell, Entwicklungs-, Test- und Betriebsumgebungen voneinander zu trennen, so dass wir ein besonderes Augenmerk hierauf haben.

Maßnahmen zur Erkennung, Vorbeugung und Wiederherstellung zum Schutz von Schadsoftware wurden getroffen und werden regelmäßig aktualisiert.

Wir verfügen über eine zentral überwachte und geschützte Ereignisprotokollierung und haben für den Fall der Speicherung sensibler personenbezogener Daten Maßnahmen zum Schutz der Privatsphäre getroffen, welche in unserem Konzept „Richtlinienkonformität“ festgelegt sind. Sämtliche Protokollierungseinrichtungen und Protokollinformationen, einschließlich Administratoren- und Bedienerprotokolle sind vor Manipulation und unbefugtem Zugriff geschützt.

Wir verfügen über ein zentrales Verfahren zur gesteuerten Installation von Software auf Systemen in unserem Unternehmen. Regelungen für die Einschränkungen von Softwareinstallationen sind von uns zentral implementiert.

Es besteht eine Aufstellung unserer technischen Werte und eine geregelte, dokumentierte Handhabung für den Fall einer technischen Schwachstelle, die u.a. unser Patch-Management mit definierten Verantwortlichkeiten umfasst.

Die Synchronisation unserer Uhren erfolgt zentral mit einer einzigen Referenzzeitquelle.
Zur Sicherung unserer Daten haben wir ein geschütztes Verfahren zur Datensicherung implementiert und dokumentiert.

Standardwartungsfenster sind definiert. Zusätzlich notwendige Fenster werden vorher angekündigt.
Im Falle einer Auditprüfung unserer Informationssysteme haben wir Maßnahmen festgelegt, die Störungen der Geschäftsprozesse soweit wie möglich minimieren.

2.9 KOMMUNIKATIONSSICHERHEIT

Als Technologieunternehmen ist die Sicherheit unserer in Netzwerken und Netzwerkdiensten gespeicherten personenbezogenen Daten und Informationen unumgänglich. Daher haben wir dokumentierte Maßnahmen umgesetzt, wie Kommunikationssicherheit in unseren Netzwerken verwaltet, gesteuert und sichergestellt wird. Die Definitionen dieser Maßnahmen sind in unserem Konzept zur Sicherheit in der Kommunikation festgelegt. Es beinhaltet zudem Richtlinien und Verfahren für die Informations- und Datenübertragung, sowie die Vereinbarungen zur Informationsübertragung an externe Stellen.

Informationsdienste, Benutzer und Informationssysteme werden bedarfsgerecht voneinander getrennt gehalten.
Unsere elektronische Nachrichtenübermittlung wird angemessen geschützt. So haben wir unter anderem Maßnahmen zum Schutz der Nachrichten vor unbefugtem Zugriff, vor Veränderung oder Denial of Service getroffen, die dem von der Organisation übernommenen Klassifizierungsschema entsprechen.

Um unsere Daten auch vertraglich nachhaltig zu schützen, schließen wir bedarfsgerechte Vertraulichkeits- oder Geheimhaltungsvereinbarungen ab, die wir regelmäßig überprüfen.

2.10 ANSCHAFFUNG, ENTWICKLUNG UND INSTANDHALTUNG VON SYSTEMEN

Es ist sichergestellt, dass Daten- und Informationssicherheit ein fester Bestandteil über den gesamten Lebenszyklus unserer Systeme ist. Dies beinhaltet auch die Anforderungen an und die Sicherung von Informationssystemen, die Dienste über öffentliche Netze bereitstellen.

Informationen, die an Transaktionen bei Anwendungsdiensten beteiligt sind, schützen wir bedarfsgerecht.

Zudem haben wir ein Verfahren zur Verwaltung von Systemänderungen eingerichtet, um die Integrität von Systemen, der Anwendungen und der Produkte von den frühen Entwurfsphasen bis zu allen später anfallenden Wartungsarbeiten sicherzustellen. Bei Änderungen an Betriebsplattformen werden geschäftskritische Anwendungen überprüft und getestet, um sicherzustellen, dass es keine negativen Auswirkungen auf die Organisationstätigkeiten oder die Organisationssicherheit gibt. Wir verfügen über einen gesteuerten Prozess zur Analyse, der Entwicklung und der Pflege sicherer IT Systeme.

Für neue Informationssysteme, Aktualisierungen und neue Versionen sind Abnahmetestprogramme und dazugehörige Kriterien festgelegt. Unsere Testdaten werden sorgfältig ausgewählt geschützt und gesteuert.

2.11 BEZIEHUNGEN ZU EXTERNEN PARTNERN

Wir wählen unsere externen Partner im Vorfeld sorgsam aus und überprüfen ihre Geeignetheit hinsichtlich der Wahrung des Daten- und Informationssicherheitsschutzes.

Dokumentierte Vereinbarungen sichern den Schutz und die Geheimhaltung unserer Werte und Daten. Sofern durch gesetzliche Vorgaben benötigt, verpflichten wir unsere externen Partner, technisch-organisatorische Maßnahmen zu treffen, um dies zu gewährleisten.

Externe Partner dürfen weitere Partner lediglich mit unserer Zustimmung beauftragen, um eine sichere Lieferkette zu gewährleisten.

Regelmäßig führen wir eine Überprüfung der Datenschutz- und Datensicherheitsmaßnahmen unserer externen Partner durch um das vereinbarte Niveau aufrecht zu erhalten. Auch die zugewiesenen Berechtigungen unterliegen einer ständigen dokumentierten Kontrolle.
Nach Beendigung des Partnerverhältnisses sind diese verpflichtet, die von uns erhaltenen Daten und Werte zu vernichten. Zudem gilt die Wahrung der Geheimhaltungspflicht unbegrenzt.

2.12 HANDHABUNG VON INFORMATIONSSICHERHEITS- UND DATENSCHUTZEREIGNISSEN

Unser Unternehmen verfügt über einen geregelten und dokumentierten Prozess für die Handhabung von Informationssicherheits- und Datenschutzvorfällen, um diesbezüglich eine konsistente und wirksame

Herangehensweise zu gewährleisten. Die Beschäftigten sind angehalten, sämtliche Datenschutz – und Sicherheitsereignisse unverzüglich zu melden und werden diesbezüglich regelmäßig geschult. Wir haben ein Meldesystem installiert, das Ereignisse an ein Interventionsteam weitergeleitet, um eine schnelle Reaktion zu gewährleisten. Sämtliche Ereignisse werden dokumentiert, klassifiziert und bewertet. Das implementierte Interventionsteam hat genaue Vorgaben, wie auf ein Ereignis zu reagieren ist.
Zusammen mit der Geschäftsführung werden regelmäßig Verbesserungsmaßnahmen besprochen und umgesetzt, die sich aus den Erkenntnissen und den gesammelten Beweisen eines Ereignisses ergeben.

2.13 INFORMATIONSSICHERHEITSASPEKTE BEIM BUSINESS CONTINUITY MANAGEMENT

Im Rahmen der Informationssicherheit wird die Verfügbarkeit von Systemen eigens bewertet und dokumentiert. Aus den Anforderungen leiten wir die technischen und organisatorischen Vorgaben, wie redundante Systeme / Anbindungen oder entsprechende Planungen ab und setzen diese konsequent und gesteuert um.

Ein übergreifender Notfallplan bildet den Rahmen bezüglich der entsprechenden Handlungsanweisungen für ausgewählte dokumentierte Notfallszenarien. Laufende aktualisierte Übungspläne für die Erprobung der eingesetzten Maßnahmen und die Dokumentation der Durchführung entsprechender Tests rundet das Notfallmanagement ab. Alle Server und Storage Systeme sind mit einer Herstellergarantie ausgestattet.

Sofern für unsere Informationssicherheit notwendig, haben wir auch unseren externen Partnern und Rechenzentrumsbetreibern alle relevanten gesetzlichen, regulatorischen, selbstauferlegten und vertraglichen Anforderungen auferlegt. Auch hier erfolgt eine regelmäßige, unabhängige Überprüfung des Informationssicherheits- und Datenschutzniveaus.

2.14 COMPLIANCE

Wir haben alle relevanten gesetzlichen, regulatorischen, selbstauferlegten oder vertraglichen Anforderungen sowie das Vorgehen unseres Unternehmens zur Einhaltung dieser Anforderungen bestimmt, dokumentiert und auf dem neuesten Stand gehalten.

Auch wurden angemessene Verfahren umgesetzt, mit denen die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten sichergestellt ist.

Um den Schutz unserer Informationen und Daten sicher zu stellen, erfolgt regelmäßig eine unabhängige Überprüfung unseres Informationssicherheit- und Datenschutzniveaus, unserer Sicherheits- und Datenschutzrichtlinien, sowie die Einhaltung von technischen Vorgaben. Jährliche Tätigkeitsberichte des Datenschutzbeauftragten dokumentieren die ergriffenen Maßnahmen.

Alle relevanten gesetzlichen, regulatorischen, selbstauferlegten und vertraglichen Anforderungen haben wir durch entsprechende Service Level Agreements auch unserem externen Rechenzentrum auferlegt. Auch hier erfolgt eine regelmäßige, unabhängige Überprüfung des Informationssicherheits- und Datenschutzniveaus.

3. Weitere Massnahmen

3.1 VERFAHRENSVERZEICHNISSE

Aktuelle Verarbeitungsübersicht bzw. Verfahrensverzeichnisse sind vorhanden.

3.2 RECHTSFOLGEABSCHÄTZUNGEN

Soweit gesetzlich gefordert, werden Verfahren vor ihrer Inbetriebnahme auf Basis vordefinierter Risikokriterien und –stufen identifiziert und den Schutzmaßnahmen gegenübergestellt. Die so getroffenen datenschutzrechtlichen Bewertungen fließen in die Umsetzung der Maßnahmen ein und werden dokumentiert.

3.3 SCHULUNG UND SENSIBILISIERUNG DER BESCHÄFTIGTEN

Beschäftigte werden regelmäßig in Fragen des Datenschutzes und der Informationssicherheit geschult und sensibilisiert.

4. Glossar

BEGRIFF	BESCHREIBUNG
Beschäftigte	Mitarbeiterinnen und Mitarbeiter der Provectus Software GmbH
Mitarbeiter	Mitarbeiterinnen und Mitarbeiter der Provectus Software GmbH inklusive freier Mitarbeiterinnen und Mitarbeiter
Benutzer	Sämtliche Personen, die Zugang zu den Systemen erhalten
Geschäftsführung	Leitung, Management der Provectus Software GmbH
IT-Sicherheit	Informationssicherheit
externe Partner	Externe Lieferanten, Geschäftspartner oder Dienstleistern
Verfahren	Als Verfahren werden einzelne Prozesse oder Prozessketten bezeichnet, welche zusätzliche durch IT-Systeme unterstützt werden können.
Personenbezogene Daten	"Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene)." Unter personenbezogene Daten fallen damit Angaben zu Namen, Matrikelnummer, Studiengang, Anschrift, Zugehörigkeiten zu Vereinigungen, etc.