Parasol Island

Allgemeine Informationssicherheits-Richtlinie

Dateiname:	02_01_PSL_ISMS_Allgemeine_ISRL_v00.10_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Justus Heinser
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	08.11.2017 | Justus Heinser
Exportiert am:	08.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	08.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	5.1 | 6.1 | 6.2 | 6.3 | 7.1 | 7.2 | 8.2 | 9.3 | 9.4 | 12.3 | 13.5

Version	Datum	Autor	Änderung
00.01	30.08.2017	Justus Heinser	Erstellung
00.02	11.09.2017	Justus Heinser	Anpassungen
00.03	12.10.2017	Peter Norenkemper	Ergänzungen
00.04	07.11.2017	Justus Heinser	Ergänzungen
00.10	08.11.2017	Justus Heinser	Finalisierung

Parasol Island

Inhaltsverzeichnis

Parasol Island

1. Einleitung

Als zielgruppenorientierte Richtlinie bietet die Allgemeine Informationssicherheits-Richtlinie allen Mitarbeitern einen zentralen und detaillierten Überblick über die gängigsten sicherheitsrelevanten Themen im Alltag.

Die Allgemeine Sicherheitsrichtlinie leitet aus den Vorgaben der Sicherheitsleitlinie konkrete organisatorische und technische Anforderungen, die für alle Projekte und Prozesse gelten. Diese Anforderungen sind die Grundlage für die Standard-Sicherheitsmaßnahmen und legen das angestrebte Sicherheitsniveau fest.

Der grundlegende Umgang mit den Parasol Island Systemen soll reglementiert werden und einen Leitfaden für jeden Benutzer über die Unternehmensstrukturen und Vorgehensweisen bieten. Viele in dieser Richtlinie aufgeführten Bereiche werden durch eigene Richtlinien noch detaillierter beschrieben.

Diese Richtlinie gilt verbindlich für alle internen und externen Mitarbeiter ohne Ausnahme. Verstöße gegen die Inhalte der Richtlinie können zu arbeitsrechtlichen Konsequenzen führen.

Auch beim Abschluss von Verträgen mit externen Dienstleistern ist darauf zu achten, dass die Vorgaben dieser Richtlinie beachtet werden. Ausnahmen von der Richtlinie sind nicht zulässig, es sei denn, sie sind in der Informationssicherheitsleitlinie ausdrücklich aufgeführt.

Durch die Veröffentlichung einer neueren Version werden alte Versionen automatisch für ungültig erklärt.

2. Rechtsvorschriften

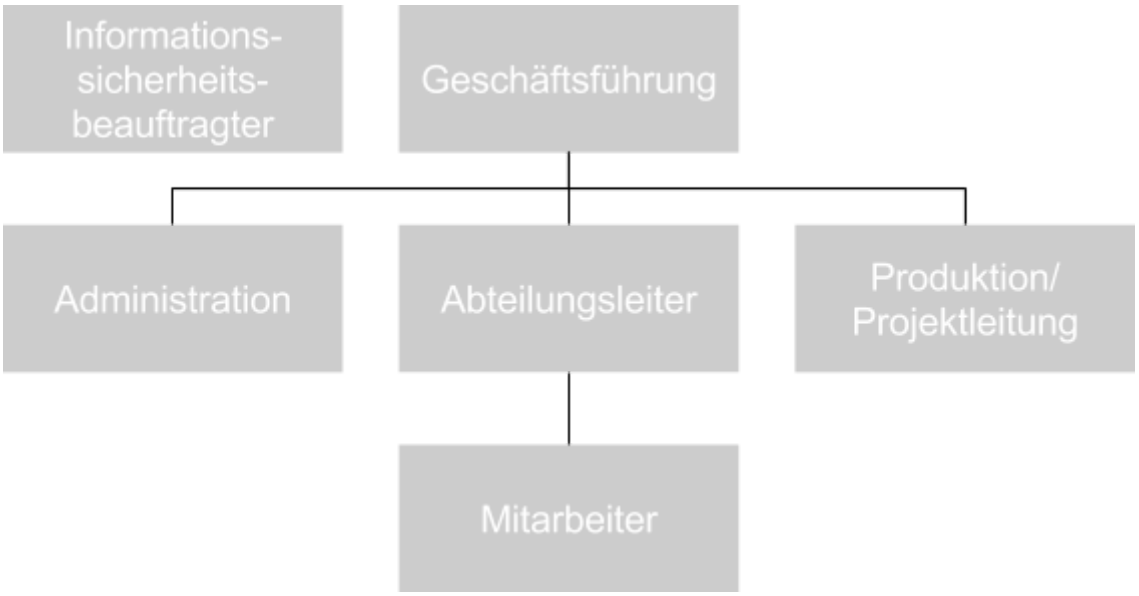
Beim Umgang mit Informationen und dem ISMS sind einschlägige Gesetze und Vorschriften einzuhalten. Beispielsweise:

- Datenschutzgesetze
- Urhebergesetze
- Arbeitnehmer Vertretungsregelungen
- Brandschutzvorschriften
- Verträge mit Kunden oder Partnern
- Aufbewahrungsfristen für Unterlagen

Weitere Dokumente hierzu:

- ➢ Richtlinie zum Schutz Personenbezogener Daten (06_02)
- ➢ Richtlinie zum Umgang mit geistigem Eigentum (02_07)

3. Organisation



Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte ist für die Pflege und Weiterentwicklung der Sicherheitsrichtlinien zuständig.
Er arbeitet zusammen mit leitenden Angestellten der verschiedenen Abteilungen Maßnahmen und Möglichkeiten aus, um die Sicherheit stetig zu verbessern.

Er definiert und kontrolliert die Sicherheitszonen innerhalb der Geschäftsräume und er definiert und kontrolliert ebenso den gesicherten Transport von Gütern und Medien, die in das Betriebsgelände eingebracht oder hinaus transportiert werden.

Der ISB führt jährlich oder nach größeren Änderungen Mitarbeiterschulungen durch und ist dafür zuständig, dass neue Mitarbeiter in die Informationssicherheitsleitlinie durch ihn oder einen seiner Stellvertreter eingeführt werden.

Der ISB ist zur Erreichung der Informationssicherheitsziele in alle IT-Projekte frühzeitig einzubeziehen. Wenn Projektziele den Sicherheitsanforderungen entgegenstehen, obliegt der Geschäftsleitung die Entscheidung, welche Anforderungen eine höhere Priorität haben.

Sicherheitsereignisse und Auffälligkeiten werden in einem Logbuch vermerkt und ausgewertet. Bei akuter Gefährdungslage oder bei Verstößen gegen die Sicherheitsrichtlinie werden alle Mitarbeiter zur Sensibilisierung im regelmäßig stattfindenden Wochenmeeting oder per Rundmail informiert.

Administrator

Die organisationsweiten IT-Dienste sind durch die bestellten Administratoren zu administrieren und zu warten. Um Sicherheitslücken zu schließen, haben sich der ISB und die Administratoren regelmäßig zu informieren. Der ISB und die Administratoren unterstützen und beraten die IT-Benutzer.

Der Administrator verwaltet das Anlegen von Benutzerkennungen und die Einrichtung der 2FA (Zwei-Faktor-Authentifizierung) Schlüssel.

Jede Administratortätigkeit ist zu loggen und zu dokumentieren und vor Veränderung im Rahmen der technischen Machbarkeit zu schützen.

Der Administrator hat in seiner Rolle nicht die Befugnis, zugriffsbeschränkte Daten einzusehen.

- ➢ Weitere Informationen finden sich in der Richtlinie für IT-Administration

Abteilungsleiter

Die Abteilungsleiter unterstützen den ISB beim Erarbeiten der Richtlinien, indem sie die Machbarkeit der Anforderungen unter dem Ziel der Informationssicherheit mit ihm erörtern. Daraus folgt eine konkrete Ausarbeitung in Form einer Arbeitsanweisung und die regelmäßige Kontrolle über die Einhaltung.

Produktion / Projektleitung

Die Produktion trägt dafür Sorge, dass die Abwicklung eines Projekts unter Einhaltung der Sicherheitsziele abläuft. Der Producer bewertet externe Dienstleister und Kunden schon vor dem Vertragsabschluss auf ihre Sicherheit. Eintreffende Informationen und Daten werden von ihm anhand der Sicherheitsstufen klassifiziert und zur Weiterverarbeitung an die berechtigten Mitarbeiter weitergereicht. Eine Risikobewertung ist in einer frühen Projektphase durchzuführen.

Weitere Informationen:

- ➢ Arbeitsanweisung zur Klassifizierung von Projekten
- ➢ Sicherheitscheckliste zur Beurteilung von Dienstleistern

Vertretungsregeln

Für den Fall der Abwesenheit (Dienstreise, Urlaub, Krankheit) sind Vertreter zu benennen, die vom Stelleninhaber einzuweisen und zu informieren sind.

4. Sensibilisierung

IT-Benutzer und Administratoren sind vor der erstmaligen Nutzung der jeweiligen IT-Dienste zu schulen. Schulungsinhalte sind:

- Handhabung der jeweilig verwendeten IT-Dienste
- Inhalte der Sicherheitsleitlinie und der Sicherheitsrichtlinien zu verschiedenen Themen sowie die umzusetzenden Sicherheitsmaßnahmen
- Sensibilisierungsmaßnahmen („Warum ist Informationssicherheit so wichtig für mich und meinen Arbeitgeber?“)
- Die Schulungen sind für alle Mitarbeiter regelmäßig zu wiederholen. Mindestens einmal im Jahr oder nach größeren Änderungen

5. Geheimhaltungsvereinbarungen

Mitarbeiter

Mitarbeiter und Freelancer sind zur Einhaltung der Informationssicherheitsrichtlinien vertraglich zu verpflichten.

Im Falle einer Bearbeitung sensibler Daten ist zusätzlich eine separate Geheimhaltungsvereinbarung abzuschließen.

Die Verpflichtungen müssen über das Arbeitsverhältnis hinausgehen und eine Vorgehensweise bei Vertragsverstößen vorgeben.

Zulieferer und Subunternehmer

Partner und Dienstleister der Parasol Island GmbH müssen in Abhängigkeit von ihrem Aufgabenbereich bzw. ihrer Auftragserfüllung ebenfalls zur Geheimhaltung verpflichtet werden.

Dies gilt besonders für Dienstleister, die Zugang zu Teilen der Sicherheitsbereiche haben. (Reinigungskräfte, Handwerker, etc.)

Besucher

Besucher müssen über die Geheimhaltung informiert werden.
Wenn Besucher Kontakt zu vertraulichem oder streng vertraulichem Material haben könnten, ist eine schriftliche Geheimhaltungsvereinbarung zu unterzeichnen.

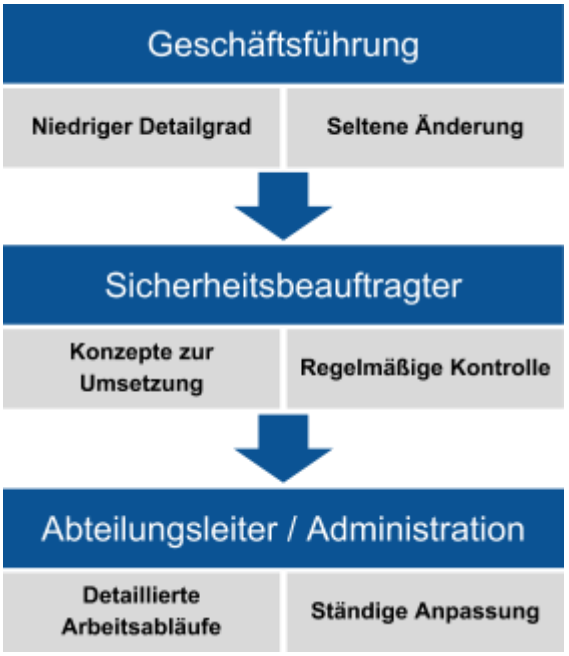
➢ Näheres regelt die Besucherregelung

6. Dokumentenebenen des ISMS

Aus zahlreichen Gründen ist die Dokumentation des Informationssicherheitsprozesses auf allen Ebenen entscheidend für dessen Erfolg. Nur durch eine ausreichende Dokumentation

- werden getroffene Entscheidungen nachvollziehbar,
- sind Prozesse wiederholbar und standardisierbar,
- können Schwächen und Fehler erkannt und zukünftig vermieden werden.

Abhängig vom Gegenstand und vom Verwendungszweck einer Dokumentation werden folgende Arten von Dokumentationen unterschieden:



01 Die Leitlinie
Die Leitlinie definiert globale Ziele und Anforderungen im Rahmen der Informationssicherheit, welche durch unterschiedliche Richtlinien, Arbeitsanweisungen und Aufzeichnungen umgesetzt werden.

- Die Genehmigung und Veröffentlichung dieser Daten und Dokumente darf nur durch die Geschäftsleitung erfolgen. Eine Delegierung ist nicht möglich.

02 Richtlinien
In den Richtlinien wird beschrieben, wie die Anforderungen aus den Leitlinien realisiert werden sollen.

- Die Berechtigung zur Prüfung, Genehmigung und Veröffentlichung hat nur der Informationssicherheitsbeauftragte der Parasol Island GmbH.

03 Arbeitsanweisungen
In den Arbeitsanweisungen werden die anzuwendenden Sicherheitsmaßnahmen in Form von Anleitungen für die Mitarbeiter verständlich dokumentiert.

- Die Berechtigung zur Prüfung, Genehmigung und Veröffentlichung aller Dokumente der dritten Ebene haben nur der Informationssicherheitsbeauftragte und die Leiter der jeweiligen Abteilungen der Parasol Island GmbH.

04 Aufzeichnungen
Aufzeichnungen müssen erstellt und instand gehalten werden, um den Nachweis der Konformität mit den Anforderungen und des wirksamen Funktionierens des ISMS zu liefern. Beispiele für Aufzeichnungen sind Managemententscheidungen, Audioaufzeichnungen, technische Dokumentationen und ausgefüllte Formulare für Zugangsberechtigungen.

- Die Klassifikation der Daten sowie die Regelung der Zugriffsberechtigung und Einhaltung der Sicherheitsvorgaben der vierten Dokumentenebene sowie aller weiteren Daten und Dokumente innerhalb der Parasol Island GmbH erfolgen durch die jeweiligen Informationseigentümer (Verantwortlichen).

7. Klassifizierung von Daten

Alle Informationen müssen anhand ihres Schutzbedarfs klassifiziert werden. Die Schutzbedarfskategorien werden vom ISB zusammen mit den Abteilungsleitern definiert und von der Leitung verabschiedet.

Der Klassifikation liegen die drei Schutzziele **Vertraulichkeit, Integrität** und **Verfügbarkeit** zugrunde. Ziel ist es, Informationen entsprechend ihres Schutzbedarfs zu verarbeiten. Aus dem Schutzbedarf der Informationen leitet sich auch der Schutzbedarf der IT-Systeme ab, auf denen die Informationen verarbeitet werden.

Alle Daten und Dokumente müssen vom jeweiligen Informationseigentümer einer dieser Stufen zugeordnet werden. Die Zuordnung muss gut lesbar und für jeden offensichtlich aus den jeweiligen Daten bzw. Dokumenten hervorgehen.

Die Höhe der Stufe richtet sich nach dem entstandenen Schaden bei Nichteinhaltung.

Vertraulichkeit

Für die Einstufung der Vertraulichkeit stellt sich die Frage: Für wen ist es notwendig, diese Daten zu sehen? Der Personenkreis, der Informationen einsehen darf, sollte so klein wie möglich gehalten werden.

Nicht gekennzeichnete Informationen werde generell als Interne Vertraulichkeitsstufe klassifiziert.

Zur Verschlüsselung ist IT-Benutzern auf Antrag ein Programm zur Verfügung zu stellen.

Vertraulichkeitsstufe Öffentlich	
Personenkreis	Daten dürfen in einem nicht veränderbaren Format (z.B. *.pdf) mit jedem geteilt werden.
Übertragung	Es gibt keine Einschränkungen hinsichtlich der Übertragung der Daten.
Speicherung	Die Daten können in beliebiger Form gespeichert und transportiert werden.
Vernichtung	Elektronische Daten können mit den Betriebssystem inhärenten Möglichkeiten gelöscht werden. Papierbasierte Daten können über den Papiermüll entsorgt werden.

Vertraulichkeitsstufe Intern	
Personenkreis	Die Daten dürfen nur von Mitarbeitern der Parasol Island GmbH eingesehen und genutzt werden. Ausnahmen können durch den Informationseigentümer oder durch ihn berechtigte Personen festgelegt werden.
Übertragung	Es gibt keine Einschränkungen hinsichtlich der Übertragung der Daten.
Speicherung	Die Daten können in beliebiger Form gespeichert und transportiert werden. Dies gilt auch für papierbasierte Daten.
Vernichtung	Elektronische Daten können mit den Betriebssystem inhärenten Möglichkeiten gelöscht werden. Papierbasierte Daten müssen über einen beliebigen Aktenvernichter entsorgt werden.

Vertraulichkeitsstufe Vertraulich	
Personenkreis	Die Daten dürfen nur von speziell berechtigten Personengruppen oder Außenstehenden eingesehen und genutzt werden. Die Festlegung der Zugriffsberechtigungen und Ausnahmen werden durch den Informationseigentümer oder speziell von ihm berechtigten Personen getroffen.
Übertragung	Die Daten dürfen innerhalb der Parasol Island GmbH unverschlüsselt übertragen werden. Eine Übertragung außerhalb der Parasol Island GmbH darf nur verschlüsselt erfolgen (verschlüsseltes VPN, verschlüsselte E-Mail, im Veracrypt Container). Die papierbasierte Übertragung außerhalb der Parasol Island GmbH darf nur in verschlossenen Umschlägen erfolgen.
Speicherung	Die Daten dürfen innerhalb der Parasol Island GmbH in beliebiger Form gespeichert und transportiert werden. Auf Datenträgern, die außerhalb der Büroräume genutzt werden, müssen die Daten verschlüsselt abgelegt werden. (z.B. Veracrypt mit AES 128 bit) Papierbasierte Daten müssen nach dem täglichen Arbeitsende in einem verschließbaren Schrank gelagert werden.
Vernichtung	Elektronische Daten müssen mit entsprechenden Programmen gelöscht werden (min. US DoD 5220.22-M (8-306. / E) (3 Passes)). Papierbasierte Daten müssen über einen Aktenvernichter (DIN 66399 Sicherheitsstufe 4) entsorgt werden.

Vertraulichkeitsstufe Streng Vertraulich	
Personenkreis	Die Daten dürfen nur vom Informationseigentümer und von ihm speziell berechtigten Personen eingesehen und genutzt werden. Die Festlegung der Zugriffsberechtigungen wird ausschließlich durch den Informationseigentümer getroffen. Die Klassifizierung ist auf jeder Seite kenntlich zu machen (Fußzeile).
Übertragung	Die Daten dürfen innerhalb der Parasol Island GmbH nur verschlüsselt übertragen werden. Eine Übertragung außerhalb der Parasol Island GmbH ist nicht zulässig. Dies gilt auch für papierbasierte Daten.
Speicherung	Die Daten dürfen innerhalb der Parasol Island GmbH nur verschlüsselt gespeichert und transportiert werden. Auf Datenträgern, die außerhalb der Büroräume genutzt werden, dürfen diese Daten nicht gespeichert werden. Die papierbasierte Aufbewahrung ist nur in verschlossenen Datenschränken zulässig.
Vernichtung	Elektronische Daten müssen mit entsprechenden Programmen gelöscht werden (Gutmann 35 Passes). Papierbasierte Daten müssen vom Informationseigentümer oder einer speziell von ihm berechtigten Person über einen Aktenvernichter (DIN 66399 Sicherheitsstufe 5) entsorgt werden.

Integrität

Wie fehlerbehaftet oder beschädigt dürfen Daten sein, ohne dass ein Schaden entsteht? Das beinhaltet auch den Schutz vor Veränderung durch Unbefugte. Kann man einen Verlust der Daten kompensieren?
Die Klassifizierung ist wichtig für das angemessene Maß der Planung von Zugriffsrechten, Schutzmaßnahmen und Einhaltung der Backup Planung.

Klasse	Beschreibung
Gering	● Eine Verletzung beeinträchtigt weder den Geschäftsbetrieb, noch das Ansehen der Firma.
Mittel	● Eine Verletzung hat nur geringe Auswirkungen und stört den Arbeitsablauf nur geringfügig. ● Schadensersatzforderungen sind unwahrscheinlich.
Hoch	● Eine Verletzung bringt merkbare Beeinträchtigungen mit sich. ● Arbeitsabläufe werden verzögert. ● Umsatzzahlen werden negativ beeinflusst. ● Kunden könnten die Zusammenarbeit beenden. ● Schadensersatzforderungen sind anzunehmen.
Sehr Hoch	● Eine Verletzung hat erhebliche Auswirkungen. ● Starke negative Auswirkung auf die Umsätze. ● Lange Ausfallzeiten in der Produktion. ● Schadensersatzforderung durch mehrere Einzelpersonen oder Organisationen sind zu erwarten.

Verfügbarkeit

Wie kritisch ist die Verfügbarkeit von IT-Systemen und Infrastruktur?

Klasse	Beschreibung
Gering	● Die Verfügbarkeit darf weniger als 95% betragen ohne dass ein nennenswerter Schaden entsteht. ● Beispiel: Intranet mit unkritischen Benutzeranwendungen.
Mittel	● Die Verfügbarkeit muss mindestens 95% betragen ● Beispiel: Firmenwiki
Hoch	● Die Verfügbarkeit muss mindestens 98% betragen. ● Produktionsrelevantes IT-System, dessen Ausfall Teilbereiche der Produktion stoppen kann. ● Beispiel: Buchhaltung, Renderfarm in unkritischen Projektphasen
Sehr Hoch	● Die Verfügbarkeit muss mindestens 99% betragen. ● Produktionsrelevantes IT-System, dessen Ausfall einen Produktionsstopp zur Folge hat. ● Beispiel: Server, Renderfarm gegen Projektende

Kontrolle

Aus den Anforderungen für die Sicherheitsziele erwächst die Notwendigkeit der Kontrolle.
Die Daten und IT-Systeme müssen entsprechend ihrer Klassifikationen Maßnahmen unterworfen werden, die einen sachgemäßen Umgang gewährleisten. Die Einhaltung der Maßnahmen muss kontrolliert werden und Änderungen müssen nachvollziehbar sein.

8. Dokumenteneigenschaften

An jedem Dokument mit einer höheren Sicherheitsklassifizierung als „Intern“ und an allen Leitlinien, Richtlinien, Verfahrensanweisungen und Aufzeichnungen sind die nachfolgenden Eigenschaften anzubringen und aktuell zu halten:

Dateiname:	Gibt den Namen an, unter dem das Dokument gespeichert wird.
Dokumentenebene:	Gibt Auskunft über die entsprechende Dokumentenebene des Dokuments (siehe Abschnitt 3).
Erstellt von:	Gibt Auskunft über den Ersteller des Dokuments.
Version:	Gibt den Versionsstand des Dokuments an.
Status:	Dokumentiert den Dokumentenstatus: Entwurf, Freigegeben, In Bearbeitung, Außer Kraft.
Letzte Aktualisierung am/von:	Dokumentiert, wer wann das entsprechende Dokument zuletzt aktualisiert hat.
Gedruckt am:	Zeigt an, wann das Dokument letztmals gedruckt wurde.
Prüfungsintervall:	Hier definiert der Informationseigentümer, in welchen Abständen das Dokument standardmäßig überprüft werden soll, um es aktuell zu halten.
Letzte Prüfung:	Datum der letzten Prüfung.
Durchgeführte Änderungen:	Hier werden die Änderungen zur vorherigen Version eingetragen.
Vertraulichkeitsklassifizierung:	Hier trägt der Informationseigentümer die Sicherheitsstufe für das Dokument ein: Öffentlich, Intern, Vertraulich, Streng Vertraulich.

9. Benutzerkennungen

Benutzerkennungen werden zentral durch die zuständige Person vergeben. Jede Person mit Zugriff auf die Parasol Island IT-Systeme, erhält eine eigene, eindeutige Benutzerkennung. Gruppenkennungen sind nicht vorgesehen.
Beispiele für Benutzerkennungen sind: Domänenzugriff, E-Mail, Intranet

Der Erhalt der Kennung und die damit einhergehende Einräumung von Rechten, sowie die Aushändigung eines 2FA Schlüssels ist vom Nutzer schriftlich zu bestätigen. Der Nutzer ist im notwendigen Umfang über die Sicherheitsregeln zu belehren.

Benutzerkennungen sind unmittelbar nach dem Verlassen der Person aus dem Unternehmen stillzulegen und der 2FA Key an die zentrale Stelle zurückzugeben.

➢ Näheres ist im Kapitel **"Regelung zur Benutzerregistrierung"** in der "**Richtlinie für IT-Administration"** aufgeführt.

10. Passwortregeln

Passwörter müssen aus Sicherheitsgründen den folgenden Anforderungen genügen:

- Passwörter müssen mindestens 10 Zeichen lang
- Aus den folgenden Zeichenklassen müssen mindestens 3 vertreten sein
    - Großbuchstaben
    - Kleinbuchstaben
    - Ziffern
    - Sonderzeichen
- Pins für Smartphones oder Tablets benötigen mindestens 6 Stellen
- Keine Wörter aus dem Lexikon oder Wörterbuch
- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter müssen geheim gehalten werden und dürfen nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte allenfalls für die Hinterlegung schriftlich fixiert werden, wobei es in diesem Fall in einem verschlossenen Umschlag sicher aufbewahrt werden muss.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.
- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.
- Passwörter, die nicht in dieses Raster fallen, werden vom System automatisch abgelehnt.

Die Passwörter müssen nach spätestens 180 Tagen gewechselt werden. Das System fordert hierzu rechtzeitig automatisch auf.

11. Mobile IT-Systeme

Um die Sicherheitseinrichtungen des Firmennetzwerkes für mobile Geräte zu nutzen, ist der Zugang über firmenfremde Netzwerke (Hotspot, Privates W-Lan) ausschließlich zum Verbindungsaufbau von VPN Verbindungen zum Firmennetzwerk zu nutzen. Ein privater Gebrauch ist ausgeschlossen.

Auf Reisen ist sicherzustellen, dass vertrauliche Daten nicht von Unbefugten eingesehen werden können. Bei Notebooks ist für diesen Zweck eine Blickschutzfolie zu benutzen, sofern im öffentlichen Raum gearbeitet wird. Der Nutzer hat darauf zu achten, dass ihm nicht über die Schulter gesehen werden kann.

Vertrauliche Daten müssen im Falle eines Verlustes so geschützt sein, dass diese nicht von Unbefugten nutzbar sind. Hierzu müssen die Daten verschlüsselt mitgeführt werden. Es empfiehlt sich eine Komplettverschlüsselung des Gerätes.

12. Clear Desk / Clean Screen

Jeder Mitarbeiter ist für die Ordnung seines Arbeitsplatzes selbst verantwortlich. Gemeinschaftsarbeitsplätze müssen konstant ordentlich gehalten werden.

Alle Dokumente der Sicherheitsstufe Vertraulich oder Streng Vertraulich müssen beim Verlassen des Arbeitsplatzes abgedeckt oder zugeklappt werden.

Zum Feierabend müssen diese Dokumente in einem verschließbaren Schrank oder Raum verstaut werden.

Bildschirme, White-Boards und andere großflächige Dokumentationsflächen dürfen nicht öffentlich einsehbar sein, wenn sie als Streng Vertraulich eingestufte Informationen enthalten. Gegebenenfalls sind die Fenster vorher zu verdunkeln. Als Vertraulich eingestufte Informationen dürfen nur so lange wie unbedingt nötig auf diesen Dokumentationsflächen sichtbar sein. Vor Besuchen von fremden Personen sind diese rechtzeitig im Vorfeld zu entfernen.

Um den Bildschirm zu sperren, ist ein Bildschirmschoner einzusetzen, der bei Verlassen des Arbeitsplatzes vom Benutzer aktiviert wird. Findet das manuelle Aktivieren nicht statt, muss sich die Sperrung nach spätestens fünf Minuten automatisch aktivieren. Bei Reaktivierung muss eine Authentifizierung erfolgen, entweder mit einem Mitarbeiterzugang oder mit einem gerätespezifischen Zugangsschutz.

Der Bildschirmschoner kann einen beliebigen Inhalt haben, darf jedoch keine schutzbedürftigen Inhalte zeigen. Ebenfalls ist darauf zu achten, dass die Inhalte für das Firmenumfeld angemessen sind (Safe-for-Work).

Diese Regelung gilt für alle Betriebsmittel der Parasol Island GmbH, für welche dies technisch möglich bzw. für den Arbeitsablauf durchführbar ist.
Automatisierte Informationsterminals und Testsysteme benötigen keinen Bildschirmschutz, sofern sie weder Daten einer Schutzstufe enthalten noch mit anderen Komponenten des Netzwerks verbunden sind.

13. Schutz vor Schadsoftware

Auf allen Arbeitsrechnern und Servern ist eine Antivirus Software zu installieren, die zentral vom Administrator gepflegt und überwacht wird. Sie überprüft regelmäßig alle Laufwerke und alle ein- und ausgehenden Daten auf Viren inklusive des E-Mail-Verkehrs. Eine Veränderung der Einstellung wird direkt vom Administrator bemerkt und behoben.

- ➢ Eine nähere Definition findet sich im Virenschutzkonzept

14. Patchmanagement

Sämtliche Arbeitsstationen sowie die dort installierten Betriebssysteme, Software, die automatische Updates unterstützen (z.B. Firefox, Flash, Chrome), sind so einzurichten, dass sie automatisch aktualisiert werden und dadurch die neuesten Sicherheitspatches enthalten.

Server- und zeitkritische Systeme werden nach vorheriger Prüfung vom Administrator aktualisiert, um einen Ausfall des Systems durch das Update auszuschließen. Dies kann bedeuten, dass in besonderen Fällen ein Testsystem verwendet oder nur eine beschränkte Menge an Systemen aktualisiert wird, um die Auswirkungen auf das restliche IT-System zu prüfen. Dies kann ggf. auch in Zusammenarbeit mit den Abteilungen geschehen.

Patches und sicherheitsrelevante Updates müssen grundsätzlich sofort installiert werden. Die einzige Ausnahme tritt dann ein, wenn der einwandfreie Betrieb der Systeme durch das Update gefährdet sein könnte. Aufgrund der vielfach verwendeten Spezialsoftware kann dies auch bedeuten, dass eine potentiell fehlerhafte Software eingesetzt wird. Dies wird in Zusammenarbeit mit den betroffenen Abteilungen diskutiert und muss abschließend von der Geschäftsleitung unter Abwägung der Risiken genehmigt werden.

- ➢ Siehe auch: Arbeitsanweisung zum Durchführen von Patches

15. Umgang mit entfernbaren Medien

Grundsätzlich ist die Verwendung von entfernbaren Medien nur für den betrieblichen Zweck erlaubt.

Die Datenträger müssen stets aufgeräumt werden und dürfen nur die Daten enthalten, die für den gerade erforderlichen Fall notwendig sind, damit beim Einsatz auf fremden Geräten keine geschützten Daten unbemerkt ausgelesen werden können. Ist ein wiederbeschreibbarer Datenträger (USB Stick) in einem fremden Gerät verwendet worden, ist dieser wie ein externer Datenträger zu behandeln und entsprechend zu prüfen.

Datenträger, die von Außenstehenden in den Betrieb kommen, müssen durch den Sicherheitsbeauftragten an einem entsprechend ausgerüsteten System auf Viren oder andere Schadprogramme hin überprüft werden. Erst dann dürfen die Daten ausgelesen und an den Verantwortlichen weitergereicht werden.

16. Umgang mit Sicherheitsereignissen

Sicherheitsereignisse sind Auffälligkeiten, die in der Erfüllung der Sicherheitsziele relevant sind.

Die Mitarbeiter sind angehalten, Auffälligkeiten an den Informationssicherheitsbeauftragten oder den Administrator zu melden. Es ist nicht erforderlich, dass auf jede Meldung hin eine Maßnahme erfolgen muss. Es liegt im Ermessen des Informationssicherheitsbeauftragten, die Ereignisse ihrer Schwere entsprechend einzusortieren (Leicht, Mittel, Hoch) und gegebenenfalls Sofortmaßnahmen einzuleiten.

Der Informationssicherheitsbeauftragte ist dazu verpflichtet, sämtliche Sicherheitsereignisse im Bereich der IT-Systeme zu erfassen und zu protokollieren sowie sich über neue Bedrohungen und Gefahren zu informieren.

Administration und ISB besprechen in regelmäßigen Abständen, jedoch mindestens einmal im Monat, die aufgetretenen Meldungen und beschließen daraufhin geeignete Maßnahmen, um auf die Ereignisse zu reagieren.

Ein Sicherheitsprotokoll wird der Geschäftsleitung regelmäßig vorgelegt.
Beispiele für Sicherheitsereignisse:

- Auftretende Störungen
- Verstöße gegen das Regelwerk
- Verdacht auf Befall mit Schadsoftware
- Auffallen von Schwachstellen von IT-Systemen