



Parasol Island

Passwort-Richtlinie

Dateiname:	02_13_PSL_ISMS_Passwort-Richtlinie_v01.00_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Justus Heinser
Version:	01.00
Status:	Freigegeben
Letzte Aktualisierung am/von:	05.12.2017 Justus Heinser
Exportiert am:	05.12.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	28.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	9.4

Version	Datum	Autor	Änderung
00.01	24.11.2017	Justus Heinser	Erstellung
00.02	27.11.2017	Justus Heinser	Anpassungen
01.00	05.12.2017	Justus Heinser	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Einleitung	2
2. Geltungsbereich	2
3. Notwendigkeit	2
4. Passwortregeln	3

1. Einleitung

Die Passwort-Richtlinie soll Informationen über die Notwendigkeit und die benötigte Komplexität der genutzten Passwörter innerhalb der Infrastruktur der Parasol Island GmbH bieten.

2. Geltungsbereich

Die Regelungen dieser Richtlinie gelten uneingeschränkt. Sie sind verbindlich und dürfen nicht umgangen werden. Ausnahmen von der Richtlinie sind nicht zulässig, es sei denn, sie sind in dieser ausdrücklich aufgeführt.

Mit Erscheinen einer neuen Version werden vorangegangene Versionen automatisch ungültig.

3. Notwendigkeit

Aufgrund der dauerhaft bestehenden Risiken wie:

- Verlust von mobilen Endgeräten
- Ungezielte und gezielte Angriffe von außen auf Parasol Island Systeme

ist neben der Verschlüsselung und einem Virens Scanner ein Sicheres Passwort in jedem einzelnen Parasol Island System erforderlich. Egal ob für das Betriebssystem, für das E-Mail-Konto, für die Agentursoftware oder jedes einzelne andere System, ist ein sicheres Passwort, welches gewisse Kriterien erfüllt, die letzte Barriere die sensible Daten vor unberechtigtem Zugriff schützt.



Parasol Island

4. 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
- 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.
- Die letzten 10 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 90 Tagen gewechselt werden. Das System fordert hierzu rechtzeitig automatisch auf.