



Parasol Island

Arbeitsanweisung zum Entfernen von Betriebsmitteln

Dateiname:	03_04_PSL_ISMS_EntfernenVonBetriebsmitteln_v00.10_jH
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Justus Heinser
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	07.11.2017 Justus Heinser
Exportiert am:	07.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	07.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	8.3 und weitere

Version	Datum	Autor	Änderung
00.01	30.08.2017	Justus Heinser	Erstellung
00.02	20.09.2017	Justus Heinser	Anpassungen
00.10	07.11.2017	Justus Heinser	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Ziel der Arbeitsanweisung zum Entfernen von Betriebsmitteln	3
2. Geltungsbereich	3
3. Mitnahme von Betriebsmitteln für geschäftliche Zwecke	3
Verschlüsselung	4
Weitergabe	4
Schnittstellen deaktivieren	4
Datensparsamkeit:	4
Einsichtnahme von Behörden auf Dienstreisen	4
4. Mitnahme in das private Umfeld	5
5. Entsorgung	5
6. Verlust	6
7. Verantwortlichkeiten	6



Parasol Island

1. Ziel der Arbeitsanweisung zum Entfernen von Betriebsmitteln

Hier soll die Handhabung von Parasol Island IT-Systemen genauer beschrieben werden, wenn diese das Betriebsgelände verlassen. Insbesondere mobile Geräte wie Tablet-Computer, Smartphones oder Notebooks sind von einem erhöhten Risiko betroffen.

Dies beinhaltet auch den Umgang oder das Verhalten, wenn das Gerät entsorgt werden muss, verloren gegangen ist oder gestohlen wurde.

Die Einschätzung des Sicherheitsrisikos und die Handhabung von mobilen und entfernbaren Geräten wird hier ebenso vorgegeben.

2. Geltungsbereich

Diese Arbeitsanweisung gilt für alle Beschäftigten der Parasol Island GmbH und für Nicht-Beschäftigte, soweit sie für Parasol Island GmbH tätig werden.

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

Diese Ausführung ersetzt weder die Richtlinie für IT-Nutzung noch andere Regelungen, sondern dient ausschließlich als ergänzende Information.

Mit Veröffentlichung einer neuen Version werden vorangegangene Versionen, die bis dahin veröffentlicht wurden, ungültig.

3. Mitnahme von Betriebsmitteln für geschäftliche Zwecke

Für Außeneinsätze gilt das dortige Einsatzgebiet als ausgeweiteter Bereich des Parasol Island Betriebsgeländes. Hierbei müssen Verantwortliche definiert werden, die für die Unversehrtheit und Sicherheit der Betriebsmittel verantwortlich sind. Diese Prüfung findet im Vorfeld für jeden Fall gesondert und unter Einbeziehung der Sicherheitseinstufung der verwendeten Daten statt.

Eine allgemeine Entfernungserlaubnis existiert für permanent überlassene Betriebsmittel, die vom Mitarbeiter ständig mitgeführt werden. Hier findet im Vorfeld eine Sicherheitsschulung statt, in der der sichere Umgang mit den Betriebsmitteln vermittelt wird. Die Verwendung von Codesperren und Pincodes muss, soweit möglich, erfolgen.



Parasol Island

Verschlüsselung

Wenn Daten auf Geräten transportiert werden, sollten diese verschlüsselt werden. Dies gilt sowohl für aktiv genutzte Geräte als auch für mobile Datenträger (USB-Sticks, mobile Festplatten etc.). Manche Geräte erlauben die Verwendung eines Festplattenkennworts – es wird empfohlen, von dieser Möglichkeit Gebrauch zu machen. Wenn der Speicher des Gerätes über Speicherkarten erweitert wird, ist auch der Inhalt dieser Karten nach Möglichkeit zu verschlüsseln.

Weitergabe

Das Gerät darf nie unbeaufsichtigt sein. Die Weitergabe des Geräts an Dritte oder Fremde ist in keinem Fall zulässig.

Schnittstellen deaktivieren

Sämtliche Funk- (WLAN, Bluetooth etc.), Infrarot- und andere Kommunikationsschnittstellen sind zu deaktivieren, sofern diese nicht benutzt werden.

Datensparsamkeit:

Wenn Daten unbedingt auf mobilen Geräten benötigt werden, sollte die Auswahl der Daten auf das Nötigste beschränkt werden. Es wird insbesondere darauf hingewiesen, dass die Speicherung von Passwörtern im Klartext nicht zulässig ist. Zudem sollten die für die Benutzer-Authentifikation und die Verschlüsselung verwendeten Passwörter in jedem Fall die derzeit gültigen Anforderungen hinsichtlich Passwortlänge und Komplexität erfüllen. Allgemeine Vorkehrungsmaßnahmen gegen Diebstahl sollten getroffen werden. (Auch in verschlossenen Fahrzeugen dürfen Geräte nicht sichtbar gelagert werden.)

Einsichtnahme von Behörden auf Dienstreisen

Bei Dienstreisen in manchen Ländern besteht die Gefahr, dass Behörden Einsicht in Daten mit erhöhter Sicherheitsklassifizierung verlangen. Je nach Reiseziel kann diese unangenehme Situation durchaus gesetzlich legitimiert sein. Da die Gesetzgebung im Konflikt mit der Vertraulichkeitsklassifizierung der Daten steht, muss im Vorfeld mit dem Informationseigner, in der Regel ein Kunde, eine Lösung für diesen Fall abgesprochen und vertraglich festgehalten werden. Während der Risikoabschätzung für Projekte ist bereits vor Vertragsabschluss vom Projektleiter die Möglichkeit einer solchen Situation zu berücksichtigen. Im Vertrag ist für diesen Fall vor allem eine Priorisierung zwischen den Sicherheitszielen Verfügbarkeit und Vertraulichkeit festzulegen, da Einzug oder Zerstörung des Geräts oder Datenträger meist eine Alternative zur Offenlegung darstellt.

Für den Fall, dass eine vertragliche Regelung im Vorfeld nicht getroffen wurde, ist die Vertraulichkeit immer zu priorisieren, auch wenn dies einen Verlust des Datenträgers bedeutet.



Parasol Island

Wenn die Möglichkeit besteht, sind die Daten bereits vor Reiseantritt verschlüsselt an den Zielort oder einen vom Zielort aus erreichbaren Server zu transferieren. In jedem Fall ist unmittelbar vor Reiseantritt oder Transfer zum Zielort ein Backup der Daten anzulegen.

Vor Reiseantritt hat der Reisende die Kontaktdaten eines vertrauten Anwalts zu erhalten, um sich im Ernstfall Rechtsbeistand einholen zu können.

Der Mitarbeiter soll den Behörden Kooperationsbereitschaft signalisieren. Zu diesem Zweck hat er ausfüllbare Geheimhaltungsvereinbarungen bei dem betreffenden Gerät mitzuführen. Für die Möglichkeit, dass sich die Mitarbeiter der Behörde zum Unterzeichnen einer Geheimhaltungsvereinbarung bereit erklären, ist diesen Einblick zu gewähren. Ein Aushändigen der Informationen ist ausgeschlossen. Das beinhaltet auch Aufzeichnungen der Informationen in allen Formen, insbesondere Fotografie, Film, Ton oder Handzeichnungen.

4. Mitnahme in das private Umfeld

Analog zur geschäftlichen Entfernung von Betriebsmitteln müssen auch bei der Mitnahme ins private Umfeld sämtliche Sicherheitsmaßnahmen erfolgen. Zusätzlich muss sichergestellt sein, dass auch im privaten Umfeld keine unberechtigten Personen Zugriff auf die enthaltenen Informationen erhalten.

Eine allgemeine Entfernungserlaubnis ist nur erteilbar, wenn die Betriebsmittel keine als Vertraulich oder Streng Vertraulich eingestuften Informationen erhalten.

Eine Entfernung von als Vertraulich oder Streng Vertraulich eingestuften Informationen ist nur nach einer Risikoeinschätzung möglich und erfordert die Genehmigung der Geschäftsleitung. Hierbei ist jeder Einzelfall separat zu prüfen und auch nur eine Ausnahmegenehmigung möglich.

5. Entsorgung

Die Entsorgung von Betriebsmitteln erfordert die Genehmigung der Geschäftsleitung.

Nicht mehr benötigte oder defekte Betriebsmittel müssen vor ihrer Entsorgung auf möglicherweise enthaltene Informationen hin überprüft werden.

Jegliche vorhandene Information, die als Intern oder höher eingestuft wurde, ist sachgemäß zu entfernen, indem nach Möglichkeit entweder die Datenträger entfernt werden (Festplatten, Flash-Speicherkarten, CDs / DVDs, etc.) oder die Datenträger mit einem geeigneten Tool mehrfach überschrieben werden.

Ist eine geeignete Löschung der Daten nicht möglich, müssen die entsprechenden Komponenten gegebenenfalls mechanisch aus dem Betriebsmittel entfernt werden. Ist eine Trennung nicht möglich,



Parasol Island

muss das Betriebsmittel, wie die Datenträger selbst auch, durch mechanische Einwirkung unlesbar gemacht werden.

6. Verlust

Geht ein Betriebsmittel verloren, während es vom Betriebsgelände entfernt wurde, muss dies umgehend dem Projektleiter und der Geschäftsleitung mitgeteilt werden. Besteht der begründete Verdacht, dass es gestohlen wurde, ist zudem die Polizei einzuschalten.

Die für die Betriebsmittel verantwortliche Person ist dazu verpflichtet, das Betriebsmittel wieder aufzufinden, sei es durch die Durchsuchung der möglichen Verlustorte, Aufsuchen von Fundbüros oder die Befragung beteiligter Kollegen oder Fremdfirmen.

Da als Vertraulich und Streng Vertraulich eingestufte Inhalte nur in verschlüsselter Form auf mobilen Betriebsmitteln gelagert werden dürfen, ist der Sicherheitsschaden über den wirtschaftlichen Schaden hinaus verhältnismäßig klein.

Für Betriebsmittel, die keine eigene Verschlüsselung bieten, ist eine erhöhte Sorgfaltspflicht erforderlich. Gemäß der Sicherheitseinstufung müssen hier ggf. mehrere verantwortliche Personen ernannt werden.

Jeder Verlust erfordert eine gesonderte Prüfung mit

- Betrachtung des Schadens,
- Gründen für den Verlust,
- Maßnahmen, um zukünftige Verluste zu verhindern.

Gegebenenfalls können Sanktionen gegen den Verantwortlichen erhoben werden.

7. Verantwortlichkeiten

Verantwortlich für die Überwachung der Entfernung von Betriebsmitteln sind die administrativen Mitarbeiter. Diese können die eigentliche Entfernung an geeignete Mitarbeiter delegieren.

Verantwortlich für die geschäftliche / private Entfernung:

- Projektleitung
- Geschäftsleitung

Verantwortlich für die Entsorgung:

- Administration