



Parasol Island

Richtlinie zum Umgang mit Fremdleistungen

Dateiname:	02_10_PSL_ISMS_Fremdleistungen_v01.00_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Justus Heinser
Version:	01.00
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:	-

Version	Datum	Autor	Änderung
00.01	30.08.2017	Justus Heinser	Erstellung
00.02	18.09.2017	Justus Heinser	Anpassungen
01.00	07.11.2017	Justus Heinser	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Zweck der Fremdleistungsrichtlinie	3
2. Geltungsbereich der Fremdleistungsrichtlinie	3
3. Einstufung	3
4. Kontrolle	4



Parasol Island

1. Zweck der Fremdleistungsrichtlinie

Die Fremdleistungsleitlinie soll Informationen zur Auswertung von durch Fremdfirmen erbrachten Leistungen in Hinblick auf die Einhaltung der Informationssicherheit liefern.

2. Geltungsbereich der Fremdleistungsrichtlinie

Diese Fremdleistungsrichtlinie gilt für alle Fremdfirmen, die für Parasol Island GmbH tätig werden.

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

3. Einstufung

Vor der Vergabe eines Projektes an eine Fremdfirma wird der Aufgabenbereich einer sicherheitstechnischen Überprüfung unterzogen. Sämtliche Informationen werden ihrer Sicherheitsstufe entsprechend aufgelistet und es wird geprüft, ob die Fremdfirma diese Informationen zur Durchführung des Projektes benötigt.

Die höchste Sicherheitsstufe für die von der Fremdfirma benötigten Informationen definiert das Mindestmaß an Sicherheit, das die Firma erfüllen muss.

Daraus geht hervor, dass eine Fremdfirma, die die Sicherheitseinstufung „Vertraulich“ und „Streng Vertraulich“ erfüllen muss, die selbe Sicherheitszertifizierung besitzen muss wie Parasol Island GmbH.

Für die Sicherheitseinstufung „Intern“ ist die vertragliche Verpflichtung zur Einhaltung der Verschwiegenheit über die Informationen erforderlich. Dies geschieht in Form einer Verschwiegenheitserklärung (NDA).

Ebenso muss das produzierte Produkt der geforderten Informationssicherheitsrichtlinie entsprechen. Hierbei geht es um die allgemeingültigen Sicherheitsnormen, denen auch die Parasol Island GmbH verpflichtet ist. Bei Serveranwendungen sind dies beispielsweise Schutz vor SQL-Injections, Cross-Site-Scripting und Einfügen von Schadcode in Dateiuploads.

4. Kontrolle

Die Zertifizierung wird durch die Kontrolle der Zertifikate seitens der Projektleitung vor Beginn der Datenübergabe durchgeführt. Eine Verschwiegenheitserklärung wird analog dazu gehandhabt. Erst nach erfolgreicher Prüfung dürfen Informationen mit erhöhter Sicherheitseinstufung an die Fremdfirma übertragen werden.

Im laufenden Projekt prüft die Projektleitung, ob die geforderten Sicherheitsmechanismen bei der Informationsübermittlung konsequent eingesetzt werden.

Auf Außeneinsätzen werden begleitende Fremdfirmen ebenfalls von der Projektleitung entsprechend beobachtet und kontrolliert.

Das Produkt wird, falls es sich um eine Anwendung handelt, während der Entwicklung, jedoch spätestens am Ende der Entwicklung einer Sicherheitsüberprüfung unterzogen. Hierbei werden Penetrationstests durchgeführt und der Quellcode in Abhängigkeit von der Projektkomplexität entweder vollständig oder in Teilen einer Sichtprüfung unterzogen.