



Parasol Island

Arbeitsanweisung zur Überprüfung von Fremdfirmen

Dateiname:	03_12_PSL_ISMS_Sicherheitsueberpfruefung_Fremdfirmen_v01.00_jH
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Philip Hansen
Version:	01.00
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:	-

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	22.09.2017	Justus Heinser	Anpassungen
01.00	08.11.2017	Justus Heinser	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Zielsetzung der Arbeitsanweisung	3
2. Grundsätze	3
3. Geheimhaltung	4
4. Fragebogen und AUDIT	4
5. Regelung der Zusammenarbeit	5



Parasol Island

1. Zielsetzung der Arbeitsanweisung

Umgang und Klassifizierung mit und von Fremdfirmen – von der ersten Kontaktaufnahme bis zur ersten Projektabwicklung. Welche Schritte sind verbindlich einzuhalten um sicher zu stellen, dass alle definierten Grundlagen der Informationssicherheitsrichtlinien von den beauftragten Fremdfirmen eingehalten werden – vor allem hinsichtlich der Anforderungen Verfügbarkeit, Vertraulichkeit und Integrität.

2. Grundsätze

Ohne das Vorliegen einer Vertraulichkeits-/Geheimhaltungsvereinbarung zwischen Auftragnehmer und Parasol Island GmbH werden keine Zutritts-/Zugangs- und/oder Zugriffsberechtigungen erteilt. Soweit Auftragnehmer Zutritts-/Zugangs- und/oder Zugriffsberechtigungen erhalten, sind diese nur im Rahmen der vereinbarten Aufgaben oder Tätigkeiten persönlich zu verwenden.

Bereitgestellte Informationen sowie Arbeitsergebnisse dürfen nicht bzw. nur nach schriftlicher Freigabe durch den autorisierten Mitarbeiter an Dritte weitergegeben werden.

Die Mitnahme von überlassenen Dokumenten, Arbeitsergebnissen, Datenträgern oder IT-Systemen außerhalb des Betriebsgeländes ist nur nach entsprechender schriftlicher Vereinbarung zulässig. Der Anschluss von fremden mobilen Geräten (z. B. USB-Stick, externe Festplatten, etc.) an Parasol Island IT-Infrastruktur ist grundsätzlich untersagt. In Ausnahmefällen – wenn dies zur Aufgabenerfüllung erforderlich ist – bedarf dies der schriftlichen Freigabe.

Schützenswerte Informationen, u. a. E-Mail-Adresse und andere personenbezogene Daten (BDSG), dürfen unabhängig vom Kommunikationsweg nur im Rahmen der geschäftlichen Notwendigkeit genutzt/weitergegeben werden.

Das Urheberrecht muss im Bedarfsfall dokumentiert werden.

Auftragnehmer dürfen nur die Bereiche betreten, die zur Erfüllung ihrer Aufgaben erforderlich sind. Auftragnehmer dürfen ohne Genehmigung durch den jeweiligen Verantwortlichen der IT kein Zugang zu IT- Systemen gewährt werden. Ausgenommen hiervon sind W-LAN Gast-Zugänge, die vom Koordinator beantragt werden können.



3. Geheimhaltung

Jeder Dienstleister unterzeichnet vor Projektbeginn die unter Anlage "04_PSL_ISMS_Freelance_Datengeheimnis" definierte Geheimhaltungsvereinbarung. Die Geheimhaltungserklärung wird spezifisch für ein Projekt erstellt und kann im Bedarfsfall ausgedehnt werden. Die Geheimhaltungserklärung ist als vertrauliches Dokument innerhalb der definierten Projektstruktur in den gesicherten Ablagebereichen abzulegen.

Diese Arbeitsanweisung gilt für alle Projekte, die als nicht vertraulich klassifiziert werden (Kriterien siehe Checkliste „Projektbewertung“).

Dienstleister, die an Projekte mitarbeiten, die den Status „vertraulich“ oder „streng vertraulich“ erhalten, werden um die Beantwortung eines Informationssicherheits-Fragebogens (siehe Anlage "04_PSL_ISMS_Checkliste_Dienstleister") gebeten (siehe Arbeitsanweisung 4)

4. Fragebogen und AUDIT

Im Falle einer bevorstehenden Beteiligung von Fremdfirmen an vertraulichen oder streng vertraulichen Projekten, ist ein Auditverfahren anzuwenden.

Der Fremdfirma wird eine Checkliste zugesendet. Hier sind alle wichtigen Fragen zur Informationssicherheit im Falle einer Projektbeteiligung bzw. Outsourcing von Projekten enthalten. Die Zusendung muss rechtzeitig vor Projektbeginn erfolgen, so dass die Fremdfirma Gelegenheit hat den Bogen rechtzeitig auszufüllen (mindestens 72 Stunden vor Projektbeginn).

Noch vor Beginn der eigentlichen Projektarbeit überprüft der Informationssicherheitsbeauftragte anhand der vorliegenden Checkliste die Angaben der Fremdfirma. Im Falle von fehlenden Angaben oder nicht zufriedenstellenden, erfolgt ein kurzfristiges Audit bei der Fremdfirma vor Ort, wiederum basierend auf der Checkliste.

Zusätzlich sind alle in der Richtlinie „Outsourcing“ definierten Punkte durch den Projektleiter oder den verantwortlichen Producer zu hinterfragen:

- Referenzen
- Kompetenz und Verfügbarkeit des Ansprechpartners
- Vertrauenswürdigkeit der Mitarbeiter
- Notfallplanung
- Zertifizierungen
- garantierte Verfügbarkeit (maximale Ausfallzeit)
- Sicherheitskonzept und Sicherheitsrichtlinien.



Parasol Island

Auf Basis der Fragenliste und das Ergebnis der Checkliste wird vor Vergabe des Projektes die Vertrauenswürdigkeit des Anbieters eingestuft – und zwar in 3 Kategorien – Vertrauenswürdig ohne Einschränkungen (nahezu 100% der Checkliste erfüllt) – Vertrauenswürdig mit Einschränkungen (nur 75% der Checkliste erfüllt) und nicht geeignet für vertrauliche Daten (unter 75% der Checkliste erfüllt).

Alle Dienstleister, die wir bei größeren, als vertraulich gekennzeichneten Vorhaben einbinden, muss eine vor-Ort Besichtigung des Outsourcing-Dienstleisters erfolgen.

5. Regelung der Zusammenarbeit

Alle sehr vertraulichen Projekte können ausschließlich in den Räumlichkeiten der Parasol Island GmbH erfolgen, einzige Ausnahmen sind Projekte, die als „vertraulich“ klassifiziert worden sind. Bei vertraulichen Projekten ist nur die Zuarbeit, nicht die Arbeit an vertraulich klassifizierten Teilbereichen des Projektes möglich.

Alle nicht vertraulichen Daten können unter Maßgabe der Geheimhaltung, Kundenschutz und Urheberschutz an den externen Dienstleister übergeben werden und müssen auch in diesem Falle nach Abwicklung des Projektes von diesem sicher gelöscht werden.

Vertrauliche Daten, wie z.B. 3D Daten des Herstellers werden grundsätzlich nur im Hause bearbeitet, jeder externe Dienstleister muss hierzu gesonderte Gast-Zugangsrechte erhalten.

Der interne Zugriff auf sehr vertrauliche Daten ist für jeden externen Dienstleister strikt untersagt und auch im Rahmen der Server Zugangsrechte nicht möglich.

Die einzige Möglichkeit des Datenzugriffes auf sehr vertrauliche Daten, ist der Zugang innerhalb eines Projekt-Teams nach dem 4- Augen Prinzip. Der interne Projektmitarbeiter überwacht den Zugriff zu jeder Zeit und das Projekt (wie z.B. die Umsetzung einer Prototypen Animation) wird mit dem externen Dienstleister gemeinsam in Form eines Teams umgesetzt. Eine unbeaufsichtigte Einzelbearbeitung ist nicht zulässig.

Hierzu ist folgendes zu berücksichtigen:

- Die Projektbearbeitung wird zu jeder Zeit überwacht
- 3D Daten können aus dem gesicherten Bereich nur durch am Projekt beteiligte interne Mitarbeiter in die 3D Software geladen werden
- Die Bearbeitung erfolgt immer nur innerhalb der dezidierten Software
- Der externe Mitarbeiter wird zu jeder Zeit beaufsichtigt
- Nach Fertigstellung des Teilbereiches des Externen werden die Daten unmittelbar wieder im geschützten Serverbereich abgelegt, dies gilt für alle weiterführenden Daten, die Prototypeninformationen enthalten oder nutzen.

Diese Anweisungen sind für alle Mitarbeiter verbindliche anzuwenden, Ausnahmen sind nur möglich, nach schriftlicher Anweisung und Risikoabwägung durch die Geschäftsleitung.