



Parasol Island

Arbeitsanweisung zur Klassifizierung von Projekten

Dateiname:	03_02_PSL_ISMS_Projektklassifizierung_v00.10_cW
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Philip Hansen
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	07.11.2017 Cedric Wolffs
Exportiert am:	07.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	07.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	6.2

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	20.09.2017	Justus Heinser	Anpassungen
00.10	07.11.2017	Cedric Wolffs	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Ziel der Arbeitsanweisung zur Sicherheitsklassifizierung von Projekten	2
2. Geltungsbereich der Arbeitsanweisung	2
3. Bezug zur Allgemeinen Sicherheitsrichtlinie	3
Vertraulichkeitsstufen	3
Zuweisen einer Klassifizierung	3
4. Risikobewertung von Projekten	3
Projekte mit hohem Schutzbedarf	4
5. Projektnachbesprechung	4
6. Umgang mit Dienstleistern	5

1. Ziel der Arbeitsanweisung zur Sicherheitsklassifizierung von Projekten

Die Arbeitsanweisung zur Klassifizierung von Projekten dient als Grundlage der Entscheidung wie mit Projekten umgegangen wird und welche Strukturen und Richtlinien zu beachten sind.

2. Geltungsbereich der Arbeitsanweisung

Die Arbeitsanweisung zur Klassifizierung von Projekten gilt für alle Mitarbeiter von Parasol Island GmbH, als auch alle projektbeteiligten Dienstleister beachten.

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

Beim Erscheinen einer neuen Version werden alle vorherigen Versionen automatisch ungültig.



Parasol Island

3. Bezug zur Allgemeinen Sicherheitsrichtlinie

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.

Vertraulichkeitsstufen

Sämtliche Informationen werden in den Stufen **Öffentlich**, **Intern**, **Vertraulich** und **Streng Vertraulich** klassifiziert.

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.

Zuweisen einer Klassifizierung

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

Nicht gekennzeichnete Informationen werden generell als Vertraulichkeitsstufe **Intern** klassifiziert.

4. Risikobewertung von Projekten

In einer frühen Projektphase ist eine Risikoeinschätzung des Projektablaufs durchzuführen und in den Projektunterlagen festzuhalten. Die genauen Anforderungen hierzu finden sich in der Risikomanagement-Richtlinie (02_12):

Wichtig ist vor allem die Identifikation von Risiken sowie die Abwägung von Wahrscheinlichkeiten und der Tragweite der Auswirkungen gegenüber den möglichen Maßnahmen.

Etablierte Standardmaßnahmen sind zu bevorzugen, um den Projektablauf möglichst vorhersehbar und reibungslos zu gestalten.



Parasol Island

Beispiele für relevante Fragen der Risikobewertung.

- Werden Zulieferer für das Projekt benötigt und erfüllen diese unsere Anforderungen an die Informationssicherheit?
- Werden freie Mitarbeiter für Spezialaufgaben oder zur Unterstützung des Teams benötigt und erfüllen diese unsere Anforderungen an die Informationssicherheit?
- Werden sensible Informationen außer Haus versendet? Und welche Übertragungswege sind möglich?
- Sind für das Projekt neue Systeme anzuschaffen oder zu organisieren (z.B. Präsentationsmedien, Messebildschirme)? Wie redundant müssen diese vorliegen? Können wir die Systeme ausgiebig vor Gebrauch testen?
- Besteht die Möglichkeit, dass auf Dienstreisen Behörden Einsicht in geheime Daten fordern könnten?
- Welche besonderen Wünsche hat der Kunde? Wie sind seine Risikoakzeptanzkriterien?

Die eingeschätzten Risiken müssen während des Projektes fortlaufend kontrolliert werden, um auf Änderungen reagieren zu können.

Projekte mit hohem Schutzbedarf

Bei Projekten mit vertraulichen oder streng vertraulichen Daten ist die vollständige Risikobewertung regelmäßig zu wiederholen. Hierfür sind im Vorfeld Milestones zu definieren, welche sich dadurch auszeichnen, dass der Arbeitsablauf sich ab dieser Projektphase ändert.

Beispiele für Milestones:

- Modellabnahme in der 3D
- Übergang von Previsualisierung zur Bildgenerierung in der 3D
- Picturelock im Storyboard
- Zwischenabnahmen
- Dreharbeiten von Realfilm

Besonders bei unplanmäßigen Änderungen im Projektablauf ist ebenfalls die vollständige Risikobewertung zu wiederholen und die Anforderungen sind an die neue Situation anzupassen.

5. Projektnachbesprechung

Nach Abschluss eines größeren Projektes ist eine Projektnachbesprechung durchzuführen, um neben dem Projektablauf auch zu überprüfen, ob alle relevanten Sicherheitsmaßnahmen eingehalten wurden. Es sind möglichst viele Projektbeteiligte in die Nachbesprechung einzubeziehen, um möglichst viele Auffälligkeiten aus allen Hierarchieebenen zur Kenntnis zu nehmen. Ziel ist es vor allem, Erkenntnisse für die Durchführung zukünftiger Projekte zu erlangen.



Parasol Island

Punkte für die Nachbesprechung können sein:

- Sind die Schutzklassen eingehalten worden?
- Sind trotz Einhaltung der Schutzklassen möglicherweise Schäden entstanden?
- Sind Risiken eingetreten, die in der vorangegangenen Risikobewertung nicht berücksichtigt wurden?
- Wie zuverlässig waren die am Projekt beteiligte Freelancer?
- Sind Projektstrukturen eingehalten worden und liegen alle Daten an den für sie vorgesehenen Orten?
- Gab es Anforderungen, die nicht durch Standardmaßnahmen abgedeckt waren?
- Ergeben sich hieraus Verbesserungsansprüche an das ISMS?

In der Nachbesprechung ist zu beschließen, wie lange das Projekt noch auf dem Arbeitsserver verbleibt, um für eventuelle Nachbesserungen noch zur Verfügung zu stehen. Nach der Lagerzeit ist das Projekt zu archivieren.

6. Umgang mit Dienstleistern

Sollten projektbezogene Aufgaben an Dienstleister ausgelagert werden, welche im gleichen Zuge Informationen einsehen müssen, sind bei einer Klassifizierung der Sicherheitsstufe *Öffentlich* keine weiteren Vorkehrungen zu treffen, als in der Allgemeinen Sicherheistrichtlinie (02_01) beschrieben.

Bei Bereitstellung von Informationen der Sicherheitsstufen *Intern*, *Vertraulich* und *Streng Vertraulich* müssen Dienstleister im Voraus die Geheimhaltungserklärung / NDA von Parasol Island, als auch die *Sicherheitscheckliste für Dienstleister* ausfüllen (04_Checkliste_Dienstleister_vXXX) und dem Projektleiter zurücksenden.

Maximal können in der Checkliste 23 Punkte erreicht werden. Für eine Klassifizierung ab *Vertraulich* sind mindestens 17 Punkte (>70%) notwendig.

In Ausnahmefällen kann durch die Projektleitung die Bereitstellung von Informationen ohne Erreichen der von 17 Punkten (<70%) beantragt werden. Dies setzt eine schriftliche Begründung, sowie eine Risiko Einschätzung voraus, welche vom Geschäftsführer zu genehmigen ist.