Parasol Island

Change Management Richtlinie

Dateiname:	02_05_PSL_ISMS_Change_Management_v00.10_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Philip Hansen
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:	12.1

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	14.09.2017	Justus Heinser	Ergänzung
00.10	07.11.2017	Justus Heinser	Finalisierung

Parasol Island

Inhaltsverzeichnis

1. Zweck der Changemanagement Richtlinie

Die Changemanagement Richtlinie soll den Umgang mit Änderungen an den IT-Systemen der Parasol Island GmbH regeln und bei dem Planungsprozess helfen.
Die Changemanagement Richtlinie gilt für alle Mitarbeiter der Parasol Island GmbH und für alle Personen, die für die Parasol Island GmbH tätig werden.

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. Risikomanagement

Vor größeren Änderungen ist eine Risikoanalyse auf Basis der Richtlinie zum Risikomanagement durchzuführen, um die Auswirkungen der Änderung auf den Betriebsablauf abzuschätzen.
Für Systeme mit erhöhtem Schutzbedarf ist eine erneute Prüfung nach vollzogener Änderung durchzuführen, in der die entstandenen Risiken neu ermittelt werden, um sicherzustellen, dass die Risikominimierung wie geplant eingetreten ist. Wenn nötig sind die Risikostrategien anzupassen, um das Risiko weiter zu senken.
Risikoeinschätzungen für bestehende Assets werden in einem Ampelsystem (1. Grün, 2. Gelb, 3. Rot) in der Assetliste festgehalten.

4. Einführung neuer Hard- oder Software

Für die Beschaffung von Hard- und Software ist als Grundlage ein Anforderungsprofil zu erstellen, das neben fachlichen und technischen Ausstattungsmerkmalen sowie ergonomischen Aspekten auch Anforderungen an die Informationssicherheit beschreibt. Nach Möglichkeit sollten Arbeitsplätze standardisiert ausgestattet werden, um Verwaltung und Administration zu erleichtern.
Es ist zu beachten, dass die Integration in die vorhandene oder geplante, informationstechnische Infrastruktur gewährleistet ist. Hierbei hat die möglichst reibungslose Funktionstüchtigkeit der IT-Komponenten oberste Priorität. Dies impliziert auch, dass Installationen gegebenenfalls auf einen Zeitraum verlegt werden, in denen keine zeitkritischen Projekte in Bearbeitung sind.
Es sind im Rahmen der Kommunikation und Archivierung bevorzugt Programme zu beschaffen, die eine Verschlüsselung ermöglichen.
Vor dem Einsatz ist neue Soft- und Hardware zu testen. Dabei sollten nach Möglichkeit Testsystem und Produktivbetrieb getrennt werden.
Es sind Test- und Freigabeverfahren zwischen der IT-Abteilung und den Fachbereichen abzusprechen. Nicht freigegebene Hard- und Software ist nicht einzusetzen.
Da durch die erforderliche Verwendung von hochspezialisierter Hard- und Software nicht sämtliche Eventualitäten oder Fehlerquellen effektiv ausgeräumt werden können, muss auch der Einsatz von fehlerbehafteten Komponenten möglich sein.
Hierzu wird in Zusammenarbeit von der IT und der Projektleitung eine Risikoeinschätzung durchgeführt und ein mögliches Vorgehen für den jeweiligen Einzelfall definiert.
Die Nutzung aller nicht ausdrücklich erlaubten Dienste ist technisch zu unterdrücken. Dienste und Berechtigungen, die nicht oder nicht mehr benötigt werden, sind durch den Administrator zu deaktivieren.
Soft- und Hardware sind durch die Administratoren möglichst so zu konfigurieren, dass ohne weiteres Zutun der IT-Benutzer optimale Sicherheit erreicht werden kann.

5. Whitelist und Blacklist

Die Black- und Whitelist soll als Hilfestellung dienen, bereits getroffene Entscheidungen über die Auswahl von IT-Systemen in Form von Software, Betriebssystemen, Programmen, Hardware, Apps, oder Webdiensten zu dokumentieren.
Da die Whitelist aufgrund der vorherrschenden Prozessstruktur als nicht vollständig zu definieren ist, wird zusätzliche eine Blacklist geführt.
Die Aufnahme in eine der Listen ist erst nach sorgfältiger Abwägung der Risiken für die Sicherheitsziele von Administration, Abteilungsleitern und Informationssicherheitsbeauftragten freizugeben.
Eine Einstufung der Software auf der Whitelist autorisiert den Nutzer nicht zur eigenmächtigen Installation ohne Einwilligung des Administrators, auch nicht bei lokalen Administratorrechten.

Installation von Raubkopien oder Software, die nicht für die Parasol Island GmbH lizenziert wurde, ist generell verboten.

6. Weiterführende Dokumente

- Risikomanagement Richtlinie (02.12)
    - Whitelist und Blacklist
        - PSL_ISMS_Whitelist_Blacklist_v00.XX_xX.gdoc
        - Zu führen vom Administrator
    - Patchplan
        - Arbeitsanweisung zu Systemupdates
        - 03_11_PSL_ISMS_Patchplan_v00.XX_xX.gdoc
        - Zu führen vom Administrator