Parasol Island

Richtlinie für IT-Administration

Dateiname:	02_02_PSL_ISMS_Administration_v01.00_jH
Dokumentenebene:	02_Richtlinie
Erstellt von:	Philip Hansen
Version:	01.00
Status:	Freigegeben
Letzte Aktualisierung am/von:	07.11.2017 | Justus Heinser
Exportiert am:	07.11.2017
Prüfungsintervall:	Halbjährlich
Letzte Prüfung:	07.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	-

Version	Datum	Autor	Änderung
00.01	22.08.2017	Philip Hansen	Erstellung
00.02	23.08.2017	Philip Hansen	Ergänzungen
00.03	30.08.2017	Justus Heinser	Ergänzungen
00.04	11.09.2017	Justus Heinser	Ergänzungen
00.05	12.10.2017	Peter Norenkemper	Ergänzungen
01.00	07.11.2017	Justus Heinser	Finalisierung

Parasol Island

Inhaltsverzeichnis

Parasol Island

1. Zweck der Richtlinie für IT-Administration

Die Richtlinie soll Regeln für Administratoren vorgeben. Sie soll den Umgang mit den Systemen regeln und vereinheitlichen.

2. Geltungsbereich der Richtlinie

Diese Richtlinie für IT-Administration gilt für alle Beschäftigten der Parasol Island GmbH und für Nicht-Beschäftigte, soweit sie für die Parasol Island GmbH tätig werden.
Die Regelungen dieser IT-Sicherheitsrichtlinie gelten uneingeschränkt. Sie sind verbindlich und dürfen nicht umgangen werden. Ausnahmen von der IT-Sicherheitsrichtlinie sind nicht zulässig, es sei denn, sie sind in der IT-Sicherheitsrichtlinie ausdrücklich aufgeführt.
Mit Erscheinen einer neueren Version werden alle veralteten Versionen automatisch ungültig.

3. Überwachung und Protokollierung

Sämtliche Zugriffe der Administratoren auf das informationsverarbeitende System sind automatisch zu protokollieren. Sollte dies nicht möglich sein, ist ein handschriftliches Protokoll anzulegen. Die Protokolle sind vor Veränderung zu schützen.
Aus den Protokolldaten muss eindeutig hervorgehen, welche Zugriffe auf die Systemdaten, die Zugriffsberechtigungsdaten und die Ereignisdaten von welchen Personen vorgenommen wurden, und welche Aktionen während des Zugriffs in Gang gesetzt wurden. Die Protokolldateien sind auf Verlangen für die Geschäftsleitung einsehbar. Die Darstellung erfolgt in lesbarer, allgemeinverständlicher Form. Andere Auswertungen sind unzulässig.

4. Remote Zugang von außen

Der Zugang zu den internen Systemen von einem externen Netzwerk ist ausschließlich über eine gesicherte VPN-Verbindung aufzubauen.

5. Netzwerkdienste

Die zentralen Netzwerkdienste DHCP, DNS und WINS sind intern eingerichtet und allein von dem zuständigen Administrator zu pflegen und aktuell zu halten. Sie sind rein vom internen Netzwerk erreichbar und technisch gegen ein Eindringen von außen geschützt.
Der E-Mail-Dienst und grundlegende Webservice-Leistungen sind ausgelagert an ein externes Unternehmen, welches durch ein SLA die Anforderungen der Parasol Island GmbH erfüllt.

6. Regelung zur Benutzerregistrierung

Jeder berechtigte Nutzer erhält eine Benutzerkennung für den Zugriff auf den Server und die Informationssysteme der Parasol Island GmbH. Die Gegebenheiten des Passworts sind unter der IT-Leitlinie zusammengefasst.

Neue Zugänge für Mitarbeiter (feste und freie Mitarbeiter, Auszubildende, Praktikanten, Volontäre, etc.) zu den IT-Systemen muss der Systemadministrator oder dessen Vertreter erstellen. Spätestens eine Woche vor Arbeitsbeginn hat er hierzu von der Personalverwaltung eine Mitteilung zu erhalten, die die folgenden Informationen enthält:

- Vorname
- Nachname
- Rolle im Unternehmen und verantwortliche Abteilung
- ggf. Hinweis, dass ein neuer Arbeitsplatz erforderlich ist
- Sicherheitseinstufung
- Beginn des Arbeitsverhältnisses
- ggf. Ende des Arbeitsverhältnisses

Auf Grundlage dieser Informationen legt der Administrator die entsprechenden Zugänge an und konfiguriert die Systeme. Hier wird auch das allgemeingültige Mitarbeiterkürzel definiert. Ein Kürzel muss eindeutig sein und darf nicht mehrfach vergeben werden. Das Kürzel besteht aus dem Anfangsbuchstaben des Vornamens und dem Nachnamen. Wurde ein Kürzel bereits vergeben, muss im Einzelfall entschieden werden.

Weitere Schritte sind:

- E-Mail-Adresse für Mitarbeiter anlegen.
- Der Mitarbeiter muss am Domainserver eingetragen werden.
- Zwei Faktor Authentifizierung Token muss eingerichtet werden. Der Erhalt ist vom neuen Mitarbeiter zu quittieren

- Der Mitarbeiter wird über seine Zugangsdaten informiert und kurz in die allgemeinen Firmenanwendungen eingeführt. Eine ausführliche Mitarbeiterschulung obliegt der jeweiligen Abteilung.
- Der neue Mitarbeiter erhält eine Sicherheitsschulung sowie das Informationssicherheitsmerkblatt und quittiert den Empfang schriftlich.

Bei Änderungen in den Personaldaten muss der Administrator entsprechend frühzeitig informiert werden.
Ebenfalls zu informieren ist er, wenn ein Mitarbeiter aus der Firma ausgeschieden ist. Die Zugänge sind daraufhin umgehend zu sperren.
Eine Sperrung von Mitarbeitern kann nur von der Geschäftsleitung beauftragt werden und muss vom Administrator durchgeführt werden.

7. Benutzerrechte auf dem Domainserver

Über die Vergabe von Benutzerrechten wird der Zugriff auf Dateien unterschiedlicher Sicherheitsklassifizierungen geregelt und kontrolliert. Der Datenbestand wird in Gruppen eingeteilt, die Benutzer dann denen für ihre Arbeit notwendigen Gruppen zugeordnet.
Daten mit der Sicherheitsklassifizierung „Intern“ werden generell allen Mitarbeitern (intern wie extern) zugänglich gemacht.
Für Projekte mit der Sicherheitsklassifizierung „Vertraulich“ bzw. „Streng Vertraulich“ wird eine eigene Gruppe definiert, um den Datenzugriff auf diese Projektdaten gesondert und exklusiv regulieren zu können.

Die folgende Übersicht zeigt die Gruppenstruktur:

Gruppenname:	Beschreibung:
Domain Users	Standard Benutzerkonten
Domain Admins	Volle Rechte zum Verwalten der Clients und Server

Passend dazu die Serverstruktur mit Zugriffsberechtigung:

Server	Zugriffsberechtigte Gruppe
\\pslsrv10	Domain Admins, Domain User
\\pslsrv17	Domain Admins, Domain User
\\pslsrv24	Domain Admins, Domain User

Die Rechtevergabe erfolgt durch die Geschäftsführung auf Basis eines dafür eingerichteten Online Formulars und wird vom Administrator eingerichtet.
Die Vergabe von Administratorenrechten erfordert die Kontrolle eines zweiten, unabhängigen Augenpaares zur Bestätigung.

8. Administratorrechte

Netzwerk / Systemadministrator

Von der Geschäftsleitung werden Systemadministratoren und Stellvertreter benannt. Die Systemadministratoren sind für den laufenden Betrieb der Informationssysteme zuständig. Die Namen der Administratoren sind in der Zuständigkeiten-Liste aufgeführt.
Der Administrator hat ausschließlich Rechte, die für seine administrierende Aufgabe notwendig sind.
Wenn möglich sollte das Administratorenkonto des Nutzers von seinem Nutzerkonto getrennt sein.
Die Administratorentätigkeit ist mit automatischen Logs zu überwachen, regelmäßig zu kontrollieren und vor Veränderung zu schützen, sofern dies technisch möglich ist.
Es gibt keine Administrations-Gruppenkonten, jedes Konto ist einer Person zuzuordnen.
Die Entscheidung, Administratorrechte zu vergeben, ist von der Geschäftsführung zu treffen. Zur Kontrolle und Risikoeinschätzung muss ein weiteres Augenpaar hinzugezogen werden (zum Beispiel Abteilungsleiter).
Die Administratorenrechte und Tätigkeit ist halbjährlich zu kontrollieren.

Lokal

In manchen Fällen ist es notwendig, einem Nutzer lokale Administratorrechte an seinem Arbeitscomputer zu gewähren. Die Autorisierung erfolgt ebenfalls durch die Geschäftsführung und ist durch ein zweites Augenpaar zu bestätigen. Der Nutzer ist vor der Vergabe über die Risiken zu informieren und hat eine besondere Sorgfaltspflicht.
Risiken sind z.B.:

- ungewollte Installation von Software, welche mit anderen Systemen interagiert und dadurch den Arbeitsablauf stört
- erhöhtes Risiko durch den Befall von Schadsoftware
- ungewolltes Löschen oder verändern von Systemdateien
- Automatische Installation von Updates oder nachgeladenen Plug-Ins, welche die Arbeitsabläufe stören.
- Versehentliches Deaktivieren von Schutzeinrichtungen

Die Rechte sind mit dem zugehörigen Computer zu dokumentieren. Lokale Administratorenrechte berechtigen nicht zum eigenmächtigen Installieren von Software.

9. Formular: Antrag zur Benutzerregistrierung

Zur Autorisierung und Protokollierung ist vor dem Einrichten der Benutzerrechte oder bei Änderungen der Antrag zur Benutzerregistrierung auszufüllen. Dieser wird als ausfüllbares *.PDF entweder von der Personalverwaltung oder der Geschäftsleitung ausgefüllt und unterschrieben an den Administrator geleitet. Die ausgefüllten Formulare werden in einem Ordner vom Administrator verwaltet. Bei der Aktualisierung wird ein bestehendes Formular durch das neue ersetzt, jedoch an das Ende des Ordners geheftet und archiviert.

Benutzerdaten

- Vorname
- Nachname
- Rolle im Unternehmen (z.B. Praktikant, Artist, Abteilungsleiter)
- Abteilung (z.B. 3D, 2D, Interactive)
- Beginn des Arbeitsverhältnisses
- Ende des Arbeitsverhältnisses
- Kürzel / Mailadresse

Zugriffsrechte

Der Nutzer wird einer vordefinierten Gruppe zugewiesen (ankreuzen). Diese ergibt sich aus der „Rolle im Unternehmen“ und der „Abteilung“.
Darüber hinaus kann Zugriff auf gesonderte Projekte mit sensiblem Schutzbedarf vergeben werden.
Die dem Mitarbeiter zugewiesene Workstation bzw. mobile Geräte werden hier eingetragen und gleichzeitig in der Inventarliste vermerkt.

Administratorrechte

Sofern dem Nutzer Administratorrechte vergeben werden, wird dies in diesem Kapitel vermerkt.
Es wird unterscheiden zwischen:

- Netzwerkadministratorrechte für das Nutzerkonto (Ausnahme)
- Vergabe eines separaten Kontos für die Netzwerkadministratorrechte mit Angabe der Nutzerkennung (Standard)
- Lokale Administratorrechte, wenn diese für den Nutzer erforderlich sind. Mit Angabe der Workstation, auf welche diese Rechte bestehen.

Hinweise:

- Administratorrechte müssen durch ein 2. Augenpaar autorisiert werden. Hierfür kann zum Beispiel der Abteilungsleiter hinzugezogen werden.
- Der Nutzer ist über die Risiken der eingeräumten Administratorrechte zu belehren.

Unterschriften

- Die Geschäftsleitung oder eine autorisierte Vertretung hat die Vergabe der Rechte durch Unterschrift zu bestätigen.
- Ein Feld für das 2. Augenpaar bei Administratorrechten.
- Der Admin hat nach Einrichtung der Rechte mit einer Unterschrift zu bestätigen.
- Der Nutzer, dem die Rechte eingeräumt werden, bestätigt den Empfang des Benutzerkontos und des Yubikeys.

Protokoll

Die regelmäßige Überprüfung der Rechte kann in einer ausgewiesenen Liste mit Datum und Unterschrift vermerkt werden. Die Prüfung der Administratorrechte wird zusätzlich vom Informationssicherheitsbeauftragten unterschrieben. Ebenso werden die vom Administrator geführten Kontrollprotokolle stichprobenartig vom ISB kontrolliert.

10. Kontrolle der Benutzerrechte

In die Vergabe der Benutzerrechte ist stichprobenartig, jedoch mindestens einmal jährlich, mit den Vorgaben abzugleichen und zu kontrollieren.
Die Administratorenrechte und Tätigkeiten sind halbjährlich zu kontrollieren. Die Kontrolle wird in einem vorgedruckten Protokoll auf dem Antrag der Benutzerrechte eingetragen, mit Datum und Unterschrift des Admins.
Die Kontrolle der Administratorrechte erfolgt durch den Informationssicherheitsbeauftragten oder die Geschäftsleitung und ist ebenfalls mit Datum und Unterschrift festzuhalten.

11. Vergabe von Benutzerrechten in der Agentursoftware

In der Agentursoftware werden Arbeitszeiten und Projektdaten sowie Adressbücher zentral verwaltet. Jeder Nutzer hat auch hier eine eindeutige Kennung. Die Zugriffsrechte auf Systembereiche und Funktionen lassen sich individuell durch Nutzergruppen einstellen, welche von der Geschäftsleitung vorgegeben sind. Derzeit nutzen wir für circa 100 Mitarbeiter ca. 20 verschiedene Nutzergruppen, welche mit der Geschäftsleitung abgestimmt, eingerichtet und zugewiesen wurden.

12. Überprüfung von Informationssystemen

In regelmäßigen Abständen, jedoch mindestens jährlich, sind die informationsverarbeitenden Systeme zu warten und auf technische Fehler zu prüfen (Systemaudit). Ziel soll es sein, die Zuverlässigkeit und somit auch die Sicherheit des Systems zu bewahren sowie Fehler zu beheben, die möglicherweise unangemessenen Datenzugriff ermöglichen.
Hierfür empfiehlt sich ein Zeitraum mit geringer Auslastung des Betriebs, zum Beispiel zwischen zwei Projekten. Der Zeitpunkt und die Dauer sind mit allen Abteilungsleitern frühzeitig abzustimmen. Die Systemnutzer sollten den Admin bei seiner Tätigkeit während des Audits nach Möglichkeit unterstützen.
Vor dem Durchführen ist der Umfang festzulegen, ein Plan mit Zielen zu erstellen und die genaue Vorgehensweise festzulegen. Die durchgeführten Diagnosen und Ergebnisse müssen protokolliert werden und der Geschäftsführung vorgelegt werden.

Zu testende Systeme:

- Lizenzserver
- Fileserver
- Renderfarm
- Firewall
- Klimaanalage
- Switches
- Workstations
- Backup und Archivierungssystem

Mögliche Tests und Diagnosen können sein:

- Sammeln von S.M.A.R.T. Daten
- Temperaturkontrollen
- Ram Test
- Kontrolle von Patches und Updates

- Kontrolle der Domänen Nutzergruppen
- Kontrolle der Inventarliste
- Portfreigaben kontrollieren
- Tiefgreifender Scan auf Schadsoftware
- Dienstleister für Klimaanlagenwartung

Mögliche Maßnahmen:

- Firmware-Updates bei Bedarf
- Erneuerung von Komponenten
- Reinigung von Computern
- Präventiv Festplatten austauschen
- Betriebssystem Neu-Installation