



Parasol Island

ISMS Leitlinie

Dateiname:	01_PSL_ISMS_Leitlinie_v00.10_pH
Dokumentenebene:	01_Leitlinie
Erstellt von:	Philip Hansen
Version:	00.10
Status:	Freigegeben
Letzte Aktualisierung am/von:	09.11.2017 Philip Hansen
Exportiert am:	09.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	09.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	-

Version	Datum	Autor	Änderung
00.01	22.08.2017	Philip Hansen	Erstellung
00.02	30.08.2017	Philip Hansen	Umsetzung in Google Docs
00.03	15.09.2017	Justus Heinser	Ergänzung
00.10	09.11.2017	Philip Hansen	Anpassung und Finalisierung zur Veröffentlichung



Parasol Island

Inhaltsverzeichnis

1. Stellenwert der Informationsverarbeitung	3
2. Begriffsdefinition	4
Bedeutung der Informationssicherheit beim Einsatz von IT	4
Informationssicherheit als Leistungsmerkmal von IT-Verfahren	5
Informationssicherheit als Leistungsmerkmal der Organisation	5
Wirtschaftlichkeit	5
Geltungsbereich	5
Sicherheit vor Verfügbarkeit	6
Prinzip des informierten Mitarbeiters	6
3. Übergreifende Ziele	6
4. Ziele im Detail	7
Verfügbarkeit	7
Vertraulichkeit	7
Integrität	7
5. Sicherungsmaßnahmen	7
Verantwortung der Geschäftsführung	7
Verantwortung der Mitarbeiter:	7
Als Straftaten kommen insbesondere in Betracht:	8
Fachverantwortliche	8
Verantwortung externer Leistungserbringer	9
6. Informationssicherheitsorganisation	9
7. Verbesserung der Sicherheit	10



1. Stellenwert der Informationsverarbeitung

Die Verarbeitung von vertraulichen Daten und Informationen spielt eine Schlüsselrolle in allen Leistungsbereichen der Parasol Island GmbH. Alle wesentlichen Prozesse werden durch Informations- und Kommunikationstechnik maßgeblich unterstützt.

Durch die verstärkte Abhängigkeit von moderner IT-Technik hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten (IT-Infrastruktur) durch vorsätzliche Angriffe von innen und außen, durch fahrlässiges Handeln, Unkenntnis oder potenzielles Versagen der Technik sowohl qualitativ als auch quantitativ deutlich erhöht.

Mangelnde Informationssicherheit kann zu Störungen bei der Aufgabenerfüllung führen, die die Leistungsfähigkeit in der Medienproduktion mindern und im Extremfall deren Geschäftsprozesse zum Erliegen bringen kann.

Vor diesem Hintergrund ist ein angemessenes Niveau der Informationssicherheit in den Geschäftsprozessen der Firmenstruktur der Parasol Island GmbH zu organisieren.

Die Verantwortung für die ordnungsgemäße und sichere Aufgabenerledigung und damit für die Informationssicherheit trägt die Geschäftsleitung (Charles Bals, Sebastian Druschel, Philip Hansen, Moritz von Schrötter).

Sie ist insbesondere verantwortlich für:

- die Schaffung organisatorischer Rahmenbedingungen zur nachhaltigen Gewährleistung von Informationssicherheit,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse,
- die Einrichtung eines Informationssicherheits-Managements,
- die Umsetzung der vereinbarten Sicherheitsmaßnahmen einschließlich der Bereitstellung der erforderlichen Betriebsmittel,
- eine hinreichende und geeignete Dokumentation der IT-Infrastruktur sowie aller Sicherheitsvorkehrungen und Sicherheitsmaßnahmen.

Die vorliegende Leitlinie beschreibt die allgemeinen Ziele, Strategien und Organisationsstrukturen, welche für die Initiierung und Etablierung eines ganzheitlichen Informationssicherheitsprozesses erforderlich sind.



2. Begriffsdefinition

Informationssicherheit bezeichnet einen Zustand, in dem die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein akzeptierbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen.

Dabei bedeuten:

- **Vertraulichkeit:** Vertrauliche Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Medieninhalte, die näheren Informationen über den Kommunikationsvorgang (wer, wann, wie lange, mit wem etc.) sowie die Daten über den Sende- und Empfangsvorgang.
- **Integrität:** Der Begriff der Integrität bezieht sich sowohl auf Informationen, Daten als auch das gesamte IT-System. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. Zum anderen bezieht sich der Begriff Integrität auch auf IT-Systeme, da die Integrität der Informationen und Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden kann.
- **Verfügbarkeit:** Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

Bedeutung der Informationssicherheit beim Einsatz von IT

Erklärtes Ziel der Parasol Island GmbH ist es, dass alle Einrichtungen, die der Erstellung, Speicherung und Übertragung von Daten dienen, so ausgewählt, integriert und konfiguriert sind, dass für die auf ihnen verarbeiteten Daten zu jeder Zeit und unter allen Umständen das angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt ist. Dies gilt auch für die Orte zur Aufbewahrung der Medien zur Datensicherung.

Die Einhaltung dieser Anforderungen ist unabdingbarer Bestandteil jedes Einsatzes von IT-Technik in den Departments ANM, FLM, INT, SLA, MEDIA sowie in allen Service Bereichen und ist mit technischen und organisatorischen Maßnahmen verbindlich sicherzustellen.



Parasol Island

Informationssicherheit als Leistungsmerkmal von IT-Verfahren

Die Informationssicherheit ist ein zu bewertendes und herbeizuführendes Leistungsmerkmal von IT-Verfahren. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist auf den IT-Einsatz zu verzichten. Belange der Informationssicherheit sind zu berücksichtigen bei

- der Entwicklung und Einführung von IT-Verfahren (neue Programme, IT-Systeme, etc.)
- dem Betrieb und der Pflege von IT-Verfahren (Dokumentation, Loggen der Zugriffe)
- der Beschaffung und Beseitigung / Entsorgung von IT-Produkten,
- der Nutzung von Diensten Dritter (externe Dienstleister).

Informationssicherheit als Leistungsmerkmal der Organisation

Technische und organisatorische Sicherheitsmaßnahmen sind so zu gestalten, dass diese stets integraler Bestandteil aller Verwaltungsprozesse sind und nicht Erweiterungen, die über das vermeintlich Notwendige hinausgehen. Belange der Informationssicherheit sind zu berücksichtigen bei

- der Gestaltung der Organisation,
- der Schaffung und Besetzung von Funktionen und Rollen,
- der Führung von Mitarbeitern,
- der Aus- und Weiterbildung,
- der Gestaltung von Arbeitsabläufen,
- der Zusammenarbeit mit anderen Dienstleistern und Externen,
- der Auswahl und dem Einsatz von Hilfsmitteln.

Wirtschaftlichkeit

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Dieser wird durch den Wert der zu schützenden Informationen und der IT-Systeme definiert. Zu bewerten sind dabei in der Regel die Auswirkungen auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens der Verwaltung und die Folgen von Gesetzesverstößen.

Für die Umsetzung der erforderlichen und angemessenen Sicherheitsmaßnahmen sind im Unternehmen die notwendigen Ressourcen (Personal, Sach- und Investitionsmittel) bereit zu stellen.

Geltungsbereich

Die Umsetzung der Maßnahmen ist verbindlich für alle Abteilungen (ANM, FLM, INT, SLA, MEDIA sowie alle Service-Bereiche). Im Unternehmen werden Sicherheitsbereiche (Zonen) eingerichtet, die Einhaltung der Zugänge und der Kontrolle der besonderen sicherheitstechnischen Vorkehrungen in diesen Bereichen obliegt der Geschäftsleitung und werden laufend durch den Informationssicherheitsbeauftragten überwacht.



Parasol Island

Die im Geltungsbereich des Unternehmens gestellten Sicherheitsanforderungen sind von übergeordnetem Interesse, für deren Umsetzung besteht eine vertragliche und gesetzliche Verpflichtung.

Sicherheit vor Verfügbarkeit

Wenn Angriffe auf die Sicherheit der IT-Infrastruktur der Parasol Island GmbH drohen oder bekannt werden oder sonstige Sicherheitsrisiken auftreten, kann die Verfügbarkeit von IT-Technik, IT-Anwendungen, Daten und Netzwerken entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten Produktion ist der Schutz vor Schäden vorrangig. Vertretbare Einschränkungen in Bedienung und Komfort sind hinzunehmen. Dies gilt in besonderem Maße für die Übergänge zu anderen Netzwerken, insbesondere zum Internet.

Prinzip des informierten Mitarbeiters

Die Mitarbeiter sind im erforderlichen Umfang bezüglich der Informationssicherheit zu sensibilisieren und zu qualifizieren.

3. Übergreifende Ziele

Unsere Daten und unsere IT-Systeme in allen Bereichen der Produktion werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau. Für Daten der Entwicklungsabteilung gelten maximale Anforderungen an die Vertraulichkeit.

Die Standard-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden.

Alle Mitarbeiter und die Unternehmensführung sind sich ihrer Verantwortung beim Umgang mit IT bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.



Parasol Island

4. Ziele im Detail

Verfügbarkeit

Für alle IT-Verfahren sind die Zeiten, in denen sie verfügbar sein sollen, festzulegen. Betriebsunterbrechungen sind in diesen Zeiten weitgehend zu vermeiden, d. h. nach Zahl und Dauer zu begrenzen. Die Beschreibung der notwendigen Verfügbarkeit umfasst

- die regelmäßigen Betriebszeiten,
- die Zeiten mit erhöhter Verfügbarkeitsanforderung,
- die maximal tolerierbare Dauer einzelner Ausfälle.

Ebenfalls festzulegen sind regelmäßig geplante Auszeiten, insbesondere zu Wartungszwecken.

Vertraulichkeit

Die in der Medienproduktion gespeicherten, verarbeiteten und weitergegebenen Daten sind vertraulich zu behandeln und jederzeit vor unbefugtem Zugriff zu schützen. Zu diesem Zweck ist für alle Daten der Personenkreis, dem der Zugriff gestattet werden soll, zu bestimmen. Der Zugriff auf IT-Systeme, IT-Anwendungen und Daten sowie Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken.

Integrität

Informationen sind gegen unbeabsichtigte Veränderung und vorsätzliche Verfälschung zu schützen. Alle IT-Verfahren sollen stets aktuelle und vollständige Informationen liefern, eventuelle verfahrens- oder informationsverarbeitungsbedingte Einschränkungen sind zu dokumentieren.

5. Sicherungsmaßnahmen

Verantwortung der Geschäftsführung

Die Geschäftsführung erlässt verbindliche Regeln zur Informationssicherheit für die Parasol Island GmbH und gibt sie den Mitarbeitern bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher.

Verantwortung der Mitarbeiter:

- Alle Mitarbeiter gewährleisten die Informationssicherheit durch verantwortungsbewusstes Handeln und halten die für die Informationssicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten IT-Systemen, Daten und Informationen um.



Parasol Island

- Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder Straftat verfolgt werden.
- Mitarbeiter, die die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährden und einen Schaden für die Verwaltung oder einen Dritten verursachen, können darüber hinaus nach den gesetzlichen Regelungen zum Schadensersatz herangezogen werden oder einem Rückgriffs-Anspruch ausgesetzt sein.

Als Straftaten kommen insbesondere in Betracht:

- das unbefugte Verschaffen von Daten anderer, die nicht für den Mitarbeiter bestimmt und die gegen den unberechtigten Zugang besonders gesichert sind,
- das Schädigen fremden Vermögens durch unrichtiges Gestalten eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugtes Verwenden von Daten oder durch unbefugtes Einwirken auf den Ablauf eines Programms,
- das rechtswidrige Löschen, Verändern, Unterdrücken und Unbrauchbarmachen von Daten,
- das unbefugte Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers oder
- strafbewehrte Verstöße gegen das Bundesdatenschutzgesetz.

Verstöße gegen die Informationssicherheit sind unverzüglich dem Informationssicherheitsbeauftragten zu melden.

Als Verstöße gelten insbesondere Handlungen, die aufgrund einer Abweichung von dieser Leitlinie oder weiteren Richtlinien zur Informationssicherheit

- der Parasol Island GmbH materielle oder immaterielle Schäden zufügen,
- den unberechtigten Zugriff auf Informationen, deren Preisgabe und / oder Änderung zulassen,
- die Nutzung von Verwaltungsinformationen für illegale Zwecke beinhalten oder
- eine Kompromittierung des Ansehens der Parasol Island GmbH zur Folge haben.

Fachverantwortliche

Für Geschäftsprozesse oder Fachverfahren sind Fachverantwortliche zu benennen, die in dem ihnen zugewiesenen Verantwortungsbereich zuständig sind für

- die Festlegung der geschäftlichen Relevanz der verarbeiteten Informationen und deren Schutzbedarf,
- die Sicherstellung, dass Verantwortlichkeiten explizit definiert und Sicherheits- und Kontrollmaßnahmen zur Verwaltung und zum Schutz der im Verantwortungsbereich befindlichen Informationen implementiert werden.

Der Fachverantwortliche muss den Zugang auf Informationen sowie den Umfang und die Art der Autorisierung definieren, die im jeweiligen Verfahren erforderlich sind. Bei diesen Entscheidungen ist zu berücksichtigen



Parasol Island

- die Notwendigkeit, die Informationen entsprechend ihrer geschäftlichen Relevanz zu schützen,
- die Aufbewahrungsvorschriften und die mit den Informationen verbundenen rechtlichen Anforderungen,
- die notwendige Zugänglichkeit der für die jeweiligen Geschäftsanforderungen erforderlichen Informationen.

Verantwortung externer Leistungserbringer

Personen und Unternehmen, die nicht zur Parasol Island GmbH gehören, für diese aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung. Dazu gehört auch, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren hat.

6. Informationssicherheitsorganisation

Als zentrale Sicherheitsinstanz der Parasol Island GmbH ernennt die Geschäftsleitung einen Informationssicherheitsbeauftragten (ISB), der für alle operativen Belange und Fragen der Informationssicherheit zuständig ist.

Es ist sicher zu stellen, dass diesem Beschäftigten ein angemessener Teil seiner Arbeitszeit für die Erledigung seiner Aufgaben als ISB zur Verfügung steht.

Die Verantwortung der einzelnen Verwaltungsbereiche für die Informationssicherheit im Rahmen ihrer Aufgabenerfüllung bleibt davon unberührt (s. Pkt. 3.1.6). Die einzelnen Verwaltungsbereiche können in ihrem Zuständigkeitsbereich eigene ISB ernennen.

Die Funktion des ISB kann auch an einen geeigneten externen Dienstleister übertragen werden.

Im jeweiligen Zuständigkeitsbereich hat der ISB folgende Aufgaben:

- Steuerung des Informationssicherheitsprozesses und Mitwirkung bei allen damit zusammenhängenden Aufgaben,
- Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,
- Erstellung, Fortschreibung und Umsetzung der sich aus dieser Leitlinie ableitenden weiteren Dokumente,
- Vorschlag von neuen Sicherheitsmaßnahmen und -strategien,
- Vertretung der Geschäftsführung in allen Angelegenheiten der Informationssicherheit,
- Ansprechpartner für die Mitarbeiter in den Fragen der Informationssicherheit,
- Koordination von Sensibilisierungs- und Schulungsmaßnahmen,
- Koordinierung und Zusammenarbeit in allen Fragen der Informationssicherheit, die sich aus dem Anschluss der Parasol Island GmbH an das kommunale Datennetz ergeben,



Parasol Island

- Meldung von besonders sicherheitsrelevanten Zwischenfällen

Bei Gefahr im Verzug ist der ISB oder sein Stellvertreter berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Dies kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzzugängen führen. Die Geschäftsleitung der Parasol Island GmbH ist hiervon unverzüglich zu unterrichten.

7. Verbesserung der Sicherheit

Der Informationssicherheitsprozess ist regelmäßig auf seine Aktualität und Wirksamkeit zu überprüfen. Insbesondere sind die Maßnahmen regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Mitarbeitern bekannt, umsetzbar und in den Betriebsablauf integrierbar sind. Die Abteilungsleiter unterstützen die ständige Verbesserung des Sicherheitsniveaus.

Die Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Informationssicherheit zu verbessern und ständig auf dem aktuellen Stand zu halten.

Düsseldorf, 09.11.2017

Unterschriften:

Philip Hansen

Sebastian Druschel

Geschäftsleitung Parasol Island GmbH