



Richtlinie für die Anforderungen an und den
Umgang mit externen IT-Dienstleistern in der
ENGAGEMENT GLOBAL gGmbH

- IT-Dienstleisterrichtlinie -

Dokumentenhistorie

Datum	Version	Änderungsgrund	Durchführend	Verantwortlich
04.06.2014	0.1	Anlegen des Dokuments	IT-SiBe	Leiter Z4
20.08.2014	0.2	Redaktionelle Überarbeitung	IT-SiBe	Leiter Z4
27.08.2014	1.0	Schlussredaktion vor Freigabe	IT-SiBe	Leiter Z4
17.08.2015	1.1	Überarbeitung nach Kommentierung S3	IT-SiBe	Leiter Z4

Freigabeerklärung

Datum 12.08.2015 durch Geschäftsführung

Inhaltsverzeichnis

1	Allgemeines	4
1.1	Zielsetzung	4
1.2	Bedeutung	4
1.3	Geltungsbereich	4
1.4	Inkrafttreten	4
2	Organisatorische Regelungen	5
2.1	Beschaffung	5
2.2	Vertrag	5
2.3	Organisation	5
2.4	Personal	6
3	Sicherheitsanforderungen	7
3.1	Allgemeine Regelungen	7
3.2	Arbeiten durch externes Personal im Hause	7
3.3	Arbeiten durch externe Dienstleister außerhalb des Hauses	7
3.4	Externe Arbeiten über Fernzugriff	7
3.5	Regelungen zum Ende der Tätigkeiten	8

Zu Grunde liegende und mit geltende Dokumente

- [1] IT-Sicherheitsleitlinie der ENGAGEMENT GLOBAL gGmbH. Stand: 01.04.2012
- [2] Richtlinie zur Organisation des IT-Sicherheitsmanagements (ISM) in der ENGAGEMENT GLOBAL gGmbH. Stand: 08/2015

1 Allgemeines

1.1 Zielsetzung

Diese Richtlinie umfasst Regelungen zur Sicherstellung der IT-Sicherheit im Falle der Beauftragung externer Unternehmen mit der Erbringung von IT-Dienstleistungen für die ENGAGEMENT GLOBAL.

IT-Dienstleistungen im Kontext dieser Richtlinie sind typischerweise

- Auslagerung von IT-gestützten Geschäftsprozessen (Outsourcing),
- Übernahme von Teilen des IT-Betriebs (Outtasking),
- Service- und Wartungsleistungen für Server, Clients und sonstige IT-Systeme oder IT-Komponenten,
- Entwicklung und Pflege von Anwendungssoftware,
- Hosting und Pflege von Webseiten,
- Betrieb eines VPN,
- Unterstützung durch betriebsfremdes Fachpersonal.

Durch die enge Verbindung zum Dienstleister und die entstehende Abhängigkeit von der Dienstleistungsqualität ergeben sich Risiken für die ENGAGEMENT GLOBAL, durch die die Geschäftstätigkeit der ENGAGEMENT GLOBAL gefährdet werden kann und ggf. auch Dritte betroffen sein können.

1.2 Bedeutung

Die Regelungen für die Anforderungen an und den Umgang mit externen IT-Dienstleistern sollen sicher stellen, dass durch die Beauftragung externer IT-Dienstleister das erreichte Niveau der IT-Sicherheit des Unternehmens nicht gefährdet wird.

1.3 Geltungsbereich

Die Richtlinie für die Anforderungen an und den Umgang mit externen IT-Dienstleistern in der ENGAGEMENT GLOBAL gilt für alle Mitarbeiter/innen in allen Betriebsstellen des Unternehmens und im Besonderen für die Abteilung Informationstechnik (Z4).

In Verträgen mit Dritten müssen entsprechende Pflichten, die sich aus dieser Richtlinie ergeben, ausdrücklich geregelt werden.

Ausnahmen von dieser Richtlinie bedürfen der schriftlichen Genehmigung durch den IT-Sicherheitsbeauftragten der ENGAGEMENT GLOBAL.

1.4 Inkrafttreten

Die Richtlinie für die Anforderungen an und den Umgang mit externen IT-Dienstleistern (IT-Dienstleisterrichtlinie) tritt ab sofort in Kraft.

2 Organisatorische Regelungen

2.1 Beschaffung

Vor jeder Entscheidung über die Beschaffung von IT-Dienstleistungen und die Beauftragung von IT-Dienstleistern sind Sicherheitsaspekte zu bedenken und bei einer Ausschreibung bzw. Beauftragung zu berücksichtigen.

Der Dienstleister ist sorgfältig auszuwählen. Fachkunde, Zuverlässigkeit und geschäftliche Seriosität sind zu prüfen.

Zu diesem Zweck sind folgende Punkte zu hinterfragen:

- Referenzen,
- Kompetenz und Verfügbarkeit des Ansprechpartners,
- Vertrauenswürdigkeit der Mitarbeiter,
- Notfallplanung,
- Zertifizierungen,
- garantierte Verfügbarkeit,
- Sicherheitskonzept und Sicherheitsrichtlinien.

Externen darf generell erst dann Zugang zu IT-Systemen und Anwendungen gewährt werden, wenn ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert.

2.2 Vertrag

Im Vertrag sind schriftlich zu vereinbaren:

- Weisungsgebundenheit des Dienstleisters,
- Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen,
- Stillschweigen über alle bekannt werdenden Informationen,
- technische und organisatorische Maßnahmen im Einflussbereich des Dienstleisters und deren Kontrolle,
- Melde- und Kommunikationswege,
- Notfallvorsorgemaßnahmen,
- Personaleinsatz durch den Dienstleister,
- Zutritts- und Zugangsrechte,
- Regelungen für den Fall der mangelhaften oder Nichterfüllung,
- Verfügbarkeitsanforderungen,
- Rechte und Pflichten des externen Personals,
- Regelungen zur Haftung,
- Verfahren bei Beendigung des Vertrags.

2.3 Organisation

Es sind auf beiden Seiten Verantwortliche zu benennen. Es ist sicherzustellen, dass diese ausreichende Befugnisse besitzen.

Externe Mitarbeiter sind vor Beginn ihrer Tätigkeit einzuweisen und über hausinterne Regelungen und Vorschriften zur IT-Sicherheit zu unterrichten.

Externe Mitarbeiter, die (eventuell) Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen und zur Verschwiegenheit zu verpflichten.

Der Dienstleister hat die Weisungen des Auftraggebers zu befolgen. Dies ist regelmäßig zu überprüfen.

Aufträge an Subunternehmer durch den Dienstleister bedürfen einer Genehmigung. Subunternehmer unterliegen den gleichen Anforderungen wie der Hauptauftragnehmer.

2.4 Personal

Externe müssen sich ausweisen.

Sofern ein Zutritt zu Sicherheitszonen, wie Rechenzentren, Server- oder Verteilerräumen zwingend erforderlich ist, sind externe Mitarbeiter zu beaufsichtigen. Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu begleiten oder zu beaufsichtigen.

Der Zugriff auf interne Daten durch Externe ist soweit wie möglich zu vermeiden. Externen kann, sofern dies zwingend erforderlich ist, ein zeitlich begrenzter Zugang gewährt werden, wenn entsprechende Sicherheitsmaßnahmen eingerichtet worden sind.

Sofern ein dauerhafter Zugang notwendig ist, sind einer namentlich benannten Person restriktive Zugangsrechte zu gewähren.

Es ist sicherzustellen, dass die externen Mitarbeiter keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.

3 Sicherheitsanforderungen

3.1 Allgemeine Regelungen

Für langfristige, umfangreiche oder komplexe IT-Dienstleistungen muss ein eigenes Sicherheitskonzept erstellt werden.

Bei Dienstleistungen zur Bereitstellung und Pflege von IT-Anwendungen sind diese Leistungen in den jeweiligen Sicherheitskonzepten der IT-Anwendungen zu berücksichtigen. Verantwortlich hierfür ist die zuständige Fachabteilung.

Die durchgeführten Arbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, evtl. Name des externen Mitarbeiters).

Eine Fehlerbeseitigung in Betriebssystemen und in systemnaher Software darf durch das externe Personal nur nach Genehmigung durch den Leiter der IT-Abteilung erfolgen.

Es sind Regelungen zur Kommunikation und zum Datenaustausch zwischen Auftraggeber und Dienstleister zu schaffen. Werden E-Mail oder andere internetbasierte Kommunikationsverfahren zum Austausch vertraulicher Informationen genutzt, sind angemessene Verschlüsselungsverfahren einzusetzen.

In Sicherheitszonen kann das Mitbringen von tragbaren IT-Systemen, Mobiltelefonen, Kameras etc. vom IT-Sicherheitsbeauftragten untersagt werden.

3.2 Arbeiten durch externes Personal im Hause

Arbeiten, die von Externen innerhalb der Räumlichkeiten der ENGAGEMENT GLOBAL stattfinden, sind nach Möglichkeit in separaten Räumlichkeiten durchzuführen.

Bei Arbeiten mit Anwendungen oder an Systemen mit hohem oder sehr hohem Schutzbedarf hat eine fachkundige Kraft die Arbeiten zu beaufsichtigen.

Externe Mitarbeiter, die über einen längeren Zeitraum in der oder für die ENGAGEMENT GLOBAL tätig sind und eventuell Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind mittels einer Vertraulichkeitsvereinbarung schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

In der Vertraulichkeitsvereinbarung ist festzulegen,

- welche Informationen vertraulich behandelt werden müssen,
- für welchen Zeitraum diese Vertraulichkeitsvereinbarung gilt,
- welche Aktionen bei Beendigung dieser Vereinbarung vorgenommen werden müssen, z.B. Vernichtung oder Rückgabe von Datenträgern,
- wie die Eigentumsrechte an Informationen geregelt sind,
- welche Regelungen für den Gebrauch und die Weitergabe von vertraulichen Informationen an weitere Partner gelten, falls dies notwendig ist,
- welche internen Regelungen und Richtlinien einzuhalten sind und
- welche Konsequenzen bei Verletzung der Vereinbarung eintreten.

3.3 Arbeiten durch externe Dienstleister außerhalb des Hauses

Wird Hardware zur Wartung oder Reparatur außer Haus gegeben, sind vorher alle vertraulichen Daten, die sich auf Datenträgern befinden, sicher zu löschen.

3.4 Externe Arbeiten über Fernzugriff

Generell ist der „Zugriff vor Ort“ dem „Fernzugriff“ vorzuziehen.

Die sichere Anbindung an das interne Netz ist zu regeln. Erfolgt der Fernzugriff über Internet, dürfen nur kryptografisch abgesicherte Protokolle mit starker Authentisierung verwendet werden.

Fernwartungszugänge dürfen nur temporär bei Bedarf geöffnet werden.

3.5 Regelungen zum Ende der Tätigkeiten

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen.

Es ist die ordnungsgemäße Funktion von gewarteten IT-Systemen zu überprüfen. Bei der Übergabe von IT-Systemen ist eine Prüfung auf Schadsoftware durchzuführen.

Sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte sind zu entziehen bzw. zu löschen. Externe Mitarbeiter sind explizit darauf hinzuweisen, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.

Daten, die im Rahmen der Leistungserbringung extern gespeichert wurden, sind nach Abschluss des Auftrags nachweislich vollständig und sicher zu löschen. Dies ist zu kontrollieren.