

Informationssicherheitsanforderungen

Erläuterung : Als Betreiber kritischer Infrastruktur ist der Auftragsgeber verpflichtet, ihre relevanten Dienstleister auf die Einhaltung der Informationssicherheitsvorgaben zu überprüfen.
Sämtliche Anforderungen beziehen sich auf Sie als Dienstleister des Auftraggebers und sind aus Perspektive Ihrer Organisation als vollständig erfüllt zu bestätigen. (Bestätigung siehe Teilnahmebedingungen Ziffer 3.1.1 Bestätigungen).

Anforderung			
ID	Kontrollziel	Beschreibung zu Kontrollziel	Gewichtung
1	Allgemeines / Organisation - Benennung eines Ansprechpartners für Informationssicherheit	Es ist ein zentraler Ansprechpartner zu benennen, der verbindliche Auskünfte zur Informationssicherheit sowohl im internen Bereich als auch im Außenverhältnis zum Auftraggeber geben kann. Bei entsprechender Unternehmensgröße können die Aufgaben auch von mehreren Mitarbeitern wahrgenommen werden. Für den Fall der Abwesenheit ist eine Vertretung sichergestellt.	Ausschlusskriterium
2	Mitarbeiter und ggf. Subdienstleister -Basis Sicherheitsüberprüfungen	Die Vertrauenswürdigkeit des Personals wird im Zuge des Einstellungsprozesses geprüft. Es wird im Einstellungsprozess eines Mitarbeiters mindestens das polizeiliche Führungszeugnis geprüft.	Ausschlusskriterium
3	Mitarbeiter und ggf. Subdienstleister - Vertraulichkeitsvereinbarung	Die Mitarbeiter sind durch ihren Arbeitsvertrag bzw. getrennte Verpflichtungserklärungen auf Vertraulichkeit und Einhaltung der datenschutzrechtlichen Bestimmungen auch über das Ende ihrer Beauftragung hinaus zu verpflichten.	Ausschlusskriterium
4	Mitarbeiter und ggf. Subdienstleister - Sicherheitsunterweisung	Die Mitarbeiter sind über die sicherheitstechnischen Anforderungen der IT-Ressourcen des Auftraggebers zu informieren. Das betrifft insbesondere die möglichen Risiken, adäquate Gegenmaßnahmen sowie die persönlichen Verantwortungen der Mitarbeiter im Rahmen ihrer Tätigkeiten. Zusätzlich sind die Mitarbeiter in Bezug auf Informationssicherheit regelmäßig durch entsprechende Schulungen oder Mitteilungen nachweislich zu unterweisen. Hierzu gehören auch sicherheitsbezogene Informationen bei Einführung neuer Techniken und Verfahren. Die Verantwortung ist jedem Mitarbeiter bewusst und die Einhaltung der Regeln und mögliche Konsequenzen bei Verstoß sind vertraglich festgehalten.	Ausschlusskriterium
5	Mitarbeiter und ggf. Subdienstleister - Ausscheiden von Mitarbeitern	Beim Ausscheiden von Mitarbeitern des Dienstleisters ist durch geeignete Maßnahmen sicherzustellen, dass der Zugriff auf Systeme und Anwendungen des Auftraggebers verhindert wird.	Ausschlusskriterium
6	Wartungssysteme und Remotezugang - Zugriffsschutz	Durch geeignete organisatorische und technische Maßnahmen ist sicherzustellen, dass nur speziell autorisierte Mitarbeiter auf den Remotezugang zugreifen können. Die Zugriffsrechte müssen so restriktiv wie möglich gehandhabt werden. Falls ein Mitarbeiter seinen Aufgabenbereich wechselt oder das Unternehmen des Dienstleisters verlässt, muss sichergestellt sein, dass ihm sofort die Zugangsberechtigung entzogen wird.	Ausschlusskriterium
7	Malwareschutz / Sicherheitsupdates - Konzept	Der Dienstleister hat wirksame Vorgaben zum Virenschutz und Patch-Management für seine IT-Einrichtungen im eigenen Hause zu etablieren, die dem Stand der Technik entsprechen und kontinuierlich der technischen Entwicklung angepasst werden.	Ausschlusskriterium
8	Malwareschutz / Sicherheitsupdates - Zeitnahes Einspielen von Sicherheitsupdates	Sicherheitsupdates für das Betriebssystem und für Kommunikationsprogramme, mit denen auf Internetdienste zugegriffen wird, müssen auf allen Systemen umgehend eingespielt werden. Insbesondere bei Firewalls und allen öffentlich erreichbaren Servern ist auf die zeitnahe Behebung von Schwachstellen Wert zu legen.	Ausschlusskriterium