Informations
Technik
Zentrum Bund

Allgemeine Sicherheitsvorgaben des ITZBund für externe Unterstützungskräfte

Die folgenden, von den internen Vorgaben im ITZBund abgeleiteten, allgemeinen Sicherheitsvorgaben gelten auch im Verhältnis zum Auftragnehmer und den von ihm eingesetzten externen Unterstützungskräften:

1. Zur Aufgabenerfüllung ist ausschließlich die Nutzung der vom ITZBund zugewiesenen IT-Systeme und IT-Dienste gestattet. Die Nutzung privater und sonstiger ITZBund-fremder IT-Systeme und IT-Dienste ist nicht gestattet. Ausnahmen hiervon bedürfen der Zustimmung der/des Informationssicherheitsbeauftragten des ITZBund. Unbeschadet der vorstehenden Regelungen können nach entsprechender Abstimmung mit dem ITZBund für die Softwareentwicklung und damit unmittelbar verbundene Aufgaben, die außerhalb des Informationsverbundes ITZBund (z.B. im Netz des Auftragnehmers) bearbeitet werden, ITZBund-fremde IT-Systeme und IT-Dienste genutzt werden.
2. Die vom ITZBund bereitgestellte Systemumgebung darf grundsätzlich nicht verändert oder analysiert werden. Dies betrifft insbesondere die voreingestellten Sicherheitsmechanismen, deren Umgehung untersagt ist. Für die Bereitstellung von Software sind standardisierte Prozesse und Tools des ITZBund zu verwenden. Eine Änderung oder Analyse der Systemumgebung ist nur dann zulässig, wenn sie Bestandteil des Auftragsgegenstands ist (z.B. Anpassung technischer Schnittstellen oder Penetrationstests). Ausgenommen hiervon sind mitwirkungspflichtige Aktualisierungen der vom ITZBund zur Verfügung gestellten Endgeräte, auf die jeweils vom ITZBund hingewiesen wird.
3. Das ITZBund kann die zur Verfügung gestellte Ausstattung jederzeit zurückfordern.
4. Es ist sicherzustellen, dass keine vertraulichen Informationen des ITZBund oder einer seiner Auftragnehmer für Unbefugte einsehbar, mithörbar oder anderweitig zugänglich sind. Mobile Arbeitsplätze sind entsprechend abzusichern. Bereitgestellte Sichtschutzfolien sind zu nutzen, wenn das Umfeld dies erfordert. Auf fernmündliche Kommunikation ist zu verzichten, wenn ein Mithören durch Unbefugte nicht ausgeschlossen werden kann. Fernmündliche Gespräche über Verschlusssachen mit Einstufung VS-NfD oder höher außerhalb der Gebäude des ITZBund und der eigenen Privatwohnung sind nicht zulässig.
5. Eine mobile Verarbeitung von Inhalten und Daten, die VS-NfD eingestuft sind, ist außerhalb der eigenen Privatwohnung bzw. Privatwohnungen von Angehörigen und bekannten Personen nur in zwingend notwendigen Fällen in Abstimmung mit dem ITZBund gestattet. Inhalte und Daten, die höher als VS-NfD eingestuft sind, dürfen nicht außerhalb der Liegenschaften des ITZBund verarbeitet werden.

6. Die Weitergabe von Informationen aus der Beschäftigung beim ITZBund an Unbefugte ist nicht gestattet, auch darf keine Kopie für eigene oder Firmenzwecke erstellt werden.
7. Vertrauliche Dokumente, Zutrittsmittel, mobile IT-Systeme und Datenträger sind sicher aufzubewahren, wenn sie nicht verwendet werden. Notebooks sind mittels Kensington-Schloss zu sichern. Smartcards zur Authentisierung sind getrennt vom zugehörigen mobilen IT-System zu verwahren.
8. Im Rahmen der Beschäftigung für das ITZBund erstellte Dokumente und sonstige Projektdaten sind auf den zentralen Datenablagen des ITZBund zu speichern und dürfen das ITZBund nicht verlassen. Eine Weitergabe von Dokumenten und sonstigen Projektdaten erfolgt nur über ITZBund-Beschäftigte.
9. Vertrauliche Informationen müssen sicher im ITZBund entsorgt werden.
10. Personenbezogene Benutzerkennungen dürfen nicht an Dritte weitergegeben werden. Es gelten die Passwortvorgaben des ITZBund, über die nach Beauftragung gesondert informiert wird.
11. Die Nutzung der vom ITZBund bereitgestellten IT-Systeme und IT-Dienste für private oder Firmenzwecke, insbesondere des Internetzugangs und des E-Mail Accounts, ist untersagt.
12. Der Datenverkehr mit dem Internet, sowie weitere Vorgänge werden automatisch protokolliert. Die Protokolldaten dienen ausschließlich zu Zwecken der Datenschutzkontrolle, der Sicherstellung eines ordnungsgemäßen Betriebes des Internetzugangs und der Aufklärung von Verstößen.
13. Private und sonstige ITZBund-fremde IoT-Geräte (Internet of Things), Wearables und digitale Assistenten dürfen nicht im Kontext der Leistungserbringung für das ITZBund genutzt werden. Für private Nutzung müssen sie während der Leistungserbringung so konfiguriert sein, dass eine Beeinträchtigung des ITZBund und seiner Beschäftigten ausgeschlossen werden kann.
14. Bei allen Tätigkeiten wird eine besondere Sorgfalt erwartet, insbesondere im Umgang mit verdächtig erscheinenden E-Mails und Dateien.
15. Festgestellte oder vermutete Informationssicherheitsvorfälle sind unverzüglich an den Service Desk (servicedesk@itzbund.de), sofern diese einen technischen Hintergrund haben, sowie an das Informationssicherheitsmanagement (sofortmeldung@itzbund.de) zu melden. Eine vom ITZBund benannte Ansprechperson ist zu informieren. Die Aufklärung eingetretener Informationssicherheitsvorfälle muss im erforderlichen Umfang unterstützt werden.

16. Im Falle der Beschädigung oder des Verlustes von Arbeitsmitteln haften die externen Unterstützungskräfte bei Vorsatz oder grober Fahrlässigkeit. Eine sofortige Meldung bei der vom ITZBund benannten Ansprechperson und beim Service Desk ist zwingend erforderlich.
17. Über diese allgemeinen Sicherheitsanweisungen hinaus sind ggf. bereichsspezifische Regelungen einzuhalten. Diese ergeben sich in der Regel durch die Sicherheitskonzeption des ITZBund und können seitens der vom ITZBund benannten Ansprechpersonen ergänzend kommuniziert werden.
18. Bei Zweifeln bzgl. der Anwendung der vorstehenden Regelungen ist Rücksprache mit den vom ITZBund benannten Ansprechpersonen zu nehmen.