

# Allgemeine Sicherheitsvorgaben des ITZBund für externe Unterstützungskräfte

1. Die Aufgabenerfüllung hat grundsätzlich innerhalb des Informationsverbundes des ITZBund und ausschließlich unter Nutzung der vom ITZBund bereitgestellten Informationstechnik (IT) zu erfolgen.
2. Wenn vertragliche Vereinbarungen zur Aufgabenerfüllung außerhalb des Informationsverbundes des ITZBund (z.B. Softwareentwicklung im Netz des Auftragnehmers und/ oder mit dessen IT-Systemen bzw. IT-Diensten) geschlossen wurden, ist die Übertragung von Informationen auf das für die Aufgabenerfüllung unbedingt erforderliche Minimum zu beschränken und darf nur hinreichend abgesichert über die dafür explizit vereinbarten Verfahren in Abstimmung mit der in der Beauftragung benannten Ansprechperson des ITZBund erfolgen.
3. ITZBund-fremde IT-Peripheriegeräte dürfen an der bereitgestellten IT nur genutzt werden, sofern die jeweilige Geräteklasse dafür vom ITZBund freigegeben ist. Eine entsprechende Übersicht kann im Bedarfsfall durch die in der Beauftragung benannte Ansprechperson des ITZBund zur Verfügung gestellt werden.
4. Die Nutzung der vom ITZBund bereitgestellten IT, inklusive der Internet- und E-Mail-Zugänge, ist für vertragsfremde Zwecke untersagt.
5. Die bereitgestellte IT, Authentisierungsmittel und Zugangskennungen dürfen nicht an andere Personen weitergegeben werden.
6. Auf der bereitgestellten IT verfügbare Softwareupdates sind unverzüglich zu installieren. Werden die vom ITZBund bereitgestellte Endgeräte nicht arbeitstäglich genutzt, muss sichergestellt werden, dass sie dennoch die notwendigen Softwareupdates erhalten. Nutzende müssen sich dazu mindestens monatlich am Endgerät anmelden und verfügbare Softwareupdates installieren.
7. Die Systemumgebung des ITZBund darf, ausgenommen von Individualisierungen der Benutzeroberflächen der bereitgestellten IT, grundsätzlich nicht verändert oder analysiert werden. Die Umgehung voreingestellter Sicherheitsmechanismen ist untersagt. 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 dies explizit Bestandteil des Auftragsgegenstands ist oder unter die Mitwirkungspflichten gemäß (6) fällt.
8. Im Rahmen des Einsatzes für das ITZBund erstellte Dokumente und sonstige Projektdaten sind auf den zentralen Datenablagen des ITZBund zu speichern.
9. Bereitgestellte IT, Zubehör und Authentisierungsmittel sind sicher aufzubewahren, wenn sie nicht verwendet werden. Notebooks sind mittels Kensington-Schloss zu sichern. Authentisierungsmittel sind getrennt vom zugehörigen Gerät zu verwahren.

10. Die Rückgabe bereitgestellter IT, Zubehör und Authentisierungsmittel ist unverzüglich aktiv zu initiieren, wenn die Aufgabenerfüllung abgeschlossen ist oder sie losgelöst davon vom ITZBund zurückgefordert wird. Sie hat grundsätzlich persönlich am ausgebenden Dienstsitz zu erfolgen. Ausnahmen sind mit der in der Beauftragung benannten Ansprechperson des ITZBund abzustimmen.
11. Es ist sicherzustellen, dass keine im Rahmen des Einsatzes beim ITZBund erlangten, vertraulichen Informationen während und nach der Beauftragung für Unbefugte einsehbar, mithörbar oder anderweitig zugänglich sind. Arbeitsplätze sind entsprechend abzusichern. Bereitgestellte Sichtschutzfolien sind bei Bedarf zu nutzen. ITZBund-fremde digitale Assistenzen dürfen nicht im Kontext der Leistungserbringung für das ITZBund genutzt werden und müssen so konfiguriert sein, dass eine Beeinträchtigung des ITZBund oder seiner Auftraggeber ausgeschlossen ist. Die Entsorgung vertraulicher Informationen in Papierform muss sicher im ITZBund vorgenommen werden.
12. Inhalte und Daten, die höher als VS-NfD eingestuft sind, werden im ITZBund nicht verarbeitet und dürfen deshalb weder innerhalb, noch außerhalb der Liegenschaften des ITZBund besprochen werden. Bei der Verarbeitung von VS-NfD muss der Grundsatz „Kenntnis nur, wenn nötig“ eingehalten werden. Gespräche über Verschlusssachen mit Einstufung VS-NfD außerhalb der Gebäude des ITZBund sind nur in zwingend notwendigen Fällen in Abstimmung mit der in der Beauftragung benannten Ansprechperson des ITZBund gestattet, wenn a) die Gespräche über Plattformen stattfinden, die für die Kommunikation von VS-NfD Inhalten zugelassen sind (bspw. Wire Bund) und b) die Nutzenden dafür Sorge tragen, dass derartige Gespräche nicht in der Öffentlichkeit stattfinden bzw. keine unbefugten Personen mithören können.
13. Bei allen Tätigkeiten wird eine besondere Sorgfalt erwartet, insbesondere im Umgang mit verdächtig erscheinenden E-Mails und Dateien. Festgestellte bzw. vermutete Informationssicherheitsvorfälle, sowie Beschädigungen oder Verlust von bereitgestellter IT, sind unverzüglich an den Service Desk ([servicedesk@itzbund.de](mailto:servicedesk@itzbund.de)) zu melden. Zusätzlich ist die in der Beauftragung benannte Ansprechperson des ITZBund zu informieren. Die Aufklärung eingetretener Informationssicherheitsvorfälle muss im erforderlichen Umfang unterstützt werden.
14. Über diese allgemeinen Sicherheitsanweisungen hinaus sind ggf. bereichs- oder themenspezifische Regelungen des ITZBund einzuhalten. Diese ergeben sich durch die Sicherheitskonzeption des ITZBund und werden, wenn relevant, seitens der in der Beauftragung benannten Ansprechperson des ITZBund ergänzend schriftlich kommuniziert, wobei E-Mail der vorgenannten Schriftform genügt.
15. Bei Zweifeln bzgl. der Anwendung der vorstehenden Regelungen ist Rücksprache mit der in der Beauftragung benannten Ansprechpersonen vom ITZBund zu nehmen.