



# CON.7 Informationssicherheit auf Auslandsreisen

## 1. Beschreibung

### 1.1. Einleitung

Berufsbedingte Reisen gehören mittlerweile zum Alltag in vielen Institutionen. Um auch außerhalb des regulären Arbeitsumfeldes arbeiten zu können, ist es dabei nötig, neben Unterlagen in Papierform auch Informationstechnik mitzuführen, wie beispielsweise Notebooks, Smartphones, Tablets, Wechselfestplatten oder USB-Sticks. Bei Geschäftsreisen, vor allem ins Ausland, gibt es jedoch eine Vielzahl an Bedrohungen und Risiken für die Informationssicherheit, die im normalen Geschäftsbetrieb nicht existieren.

Jede Reise ist individuell zu bewerten, da sich aufgrund der Kombination aus Reisezweck (geschäftliche Besprechung, Tagung, Kongress etc.), Reisedauer und Reiseziel jeweils eine neue Bedrohungslage ergibt, auch in Bezug auf den Schutz geschäftskritischer Informationen.

Die Bedrohungslage ist auf Reisen besonders erhöht. Dies ergibt sich z. B. aus der Kommunikation über öffentliche Netze, die nicht unter der Kontrolle der eigenen Institution stehen. Dadurch werden etwa Gefahren erneut relevant, gegen die sich die Institution vielleicht schon abgesichert hat. Hinzu kommt, dass das Risiko auf Auslandsreisen abhängig vom Zielland oftmals deutlich höher ist als bei Reisen im Inland.

Der Schutz betrieblicher und dienstlicher Informationen ist aufgrund ständig wechselnder Reiseziele, sowie regulatorischer und gesetzlicher Anforderungen, nicht immer einfach zu realisieren. So können z. B. gesetzliche Anforderungen die Einreisekontrolle verschärfen und somit den Schutz der Vertraulichkeit von Daten beeinflussen. Damit ergeben sich abhängig von Art und Dauer der Reise, sowie dem Reiseziel, individuelle Anforderungen an die Informationssicherheit. Politische, gesellschaftliche, religiöse, geografische, klimatische, gesetzliche und regulatorische Besonderheiten einzelner Reiseziele spielen hier eine maßgebliche Rolle.

### 1.2. Zielsetzung

Dieser Baustein beschreibt den Schutz aller Informationen, die auf Auslandsreisen sowohl in elektronischer als auch in physischer Form mitgeführt werden, in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit. Vertrauliche Informationen, die reisende Mitarbeitende im Kopf mitführen, sind ebenfalls Gegenstand dieses Bausteines. Es werden angemessene Regelungen und Maßnahmen für den Umgang mit schützenswerten Informationen und Daten auf Auslandsreisen aufgezeigt. Zu

berücksichtigen sind dabei grundsätzliche Rahmenbedingungen, etwa aus den Bereichen IT, Datenschutz und Recht.

In diesem Baustein werden Gefährdungen und Anforderungen spezifischer Szenarien herausgestellt, die in direktem Zusammenhang mit dem sicheren Einsatz von Informationstechnik, den Informationen und den eingesetzten Geräten auf Auslandsreisen stehen.

Dieser Baustein dient den Verantwortlichen einer Institution als Orientierungshilfe, um angemessene Sicherheitsmaßnahmen im Rahmen der Informationssicherheit auf Auslandsreisen zu etablieren. Dabei werden die wesentlichen Grundsätze aufgezeigt, die in diesem Zusammenhang zu berücksichtigen sind. Viele der genannten Gefährdungen gelten auch bei Reisen im Inland oder grundsätzlich bei der Verarbeitung von Informationen in Umgebungen, die nicht unter Kontrolle der eigenen Institution stehen.

### 1.3. Abgrenzung und Modellierung

Der Baustein CON.7 *Informationssicherheit auf Auslandsreisen* ist für den Informationsverbund anzuwenden, wenn Mitarbeitende ins Ausland reisen oder zeitweise im Ausland tätig sind und dabei besonders schutzbedürftige Informationen mitgeführt oder verarbeitet werden.

Der Baustein umfasst grundsätzlich die Anforderungen, die zu einem angemessenen Schutz von Informationen auf Auslandsreisen beitragen. Dabei hat der Schutz der Vertraulichkeit und der Integrität von schützenswerten Informationen auf Reisen den gleichen Stellenwert wie am Sitz der Institution.

Gefährdungen und Anforderungen, die den lokalen Informationsverbund betreffen, werden hier nicht betrachtet.

Da im Baustein CON.7 *Informationssicherheit auf Auslandsreisen* speziell die prozessualen, technischen und organisatorischen Anforderungen betrachtet werden, die spezifisch für die geschäftliche Arbeit auf Reisen sind, werden Anforderungen der Schichten NET *Netze und Kommunikation*, SYS *IT-Systeme* und APP *Anwendungen* nicht betrachtet. Alle notwendigen Bausteine, vor allem SYS.2.1 *Allgemeiner Client*, NET.3.3 *VPN* und SYS.3.2.2 *Mobile Device Management (MDM)*, müssen gesondert berücksichtigt werden.

Zudem sind die Anforderungen aus den thematisch ähnlichen Bausteinen INF.9 *Mobiler Arbeitsplatz* und OPS.1.2.4 *Telearbeit* zu beachten und umzusetzen.

Innerhalb dieses Bausteins kommt es außerdem zu Überschneidungen mit weiteren Bausteinen und Themenfeldern, die hier nicht betrachtet werden:

- Erfüllung der Datenschutzanforderungen,
- Präventive Maßnahmen zum Schutz von Informationen (auch technische Anforderungen, die an tragbare IT-Systeme gestellt werden, z. B. Abstrahl- oder Abhörschutz) sowie
- Personelle Sicherheit.

## 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbände eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.7 *Informationssicherheit auf Auslandsreisen* von besonderer Bedeutung.

## 2.1. Abhören und Ausspähen von Informationen/Wirtschaftsspionage

Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Institutionen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Insbesondere bei Reisen ins Ausland gibt es unbekannte Gefahrenquellen, auf die das Informationssicherheitsmanagement der eigenen Institution keinen Einfluss hat. Grundsätzlich bestehen in fremden Räumen und fremden IT-Umgebungen viele Gefahren durch das gezielte Abhören von Unterhaltungen, Leitungen, Telefongesprächen oder Datenübertragungen. Dies kann vor allem im Ausland durch entsprechende rechtliche Möglichkeiten problematisch und für die Reisenden nur schwer einschätzbar sein.

Die Gefährdungen können öffentliche Plätze und Räume betreffen, Gegebenheiten in anderen Institutionen, aber auch institutionseigene Repräsentanzen im Ausland. Auch Geräte, wie z. B. Mobiltelefone, können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Zudem sind viele IT-Systeme standardmäßig mit Mikrofon und Kameras ausgestattet, die angegriffen und dann ausgenutzt werden können.

Darüber hinaus kann es bei bestimmten Ländern Restriktionen bei der Ein- und Ausreise geben, die regulatorische Vorgaben des Herkunftslandes und Anforderungen der Institution an die Sicherheit außer Kraft setzen bzw. diesen widersprechen. Zum Beispiel kann Einsicht in Daten verlangt werden, die auf Notebooks und anderen tragbaren IT-Systemen gespeichert sind. Hierbei können zum Teil vertrauliche und personenbezogene Daten nicht nur eingesehen, sondern auch kopiert und gespeichert werden. Da es sich bei diesen Informationen z. B. auch um Strategiepapiere oder streng vertrauliche Entwürfe einer Institution handeln könnte, muss bei einer Einsichtnahme immer mit einem potenziellen Missbrauch gerechnet werden (Wirtschaftsspionage).

Auf Auslandsreisen besteht nicht nur die Gefahr, dass Informationen auf technisch komplexem Weg abgehört werden können. Oft können schützenswerte Daten auf optischem, akustischem oder elektronischem Weg einfacher ausgespäht werden, da im Ausland häufig nicht die gewohnten Ansprüche an informationssicherheitstechnische Bestimmungen gestellt werden können. Dies betrifft z. B. das allgemeine Sicherheitslevel eines Landes sowie die Gegebenheiten vor Ort, die Reisende zwangsläufig nutzen müssen.

## 2.2. Offenlegung und Missbrauch schützenswerter Informationen (elektronisch und physisch)

Beim Austausch von Informationen kann es vorkommen, dass neben den gewünschten Informationen auch ungewollt schutzbedürftige Informationen übermittelt werden. Das kann sowohl beim elektronischen Versenden von Informationen als auch während eines Telefonats oder bei der persönlichen Übergabe von Datenträgern geschehen. Auf Auslandsreisen wird der sichere Informationsaustausch aufgrund von technisch unsicheren Gegebenheiten zum Teil noch weiter erschwert. Zudem kann es vorkommen, dass Geschäftsreisende vertrauliche Dokumente sowohl physischer als auch elektronischer Art in öffentlichen Räumen oder im Hotelzimmer aus Unachtsamkeit offen einsehbar liegen lassen.

Die Kommunikation mit unbekanntem IT-Systemen und Netzen birgt immer ein Gefährdungspotenzial für das eigene Endgerät. So können z. B. auch vertrauliche Informationen kopiert werden.

Auf der anderen Seite können fremde Datenträger auch Schadprogramme enthalten. Hier besteht die Gefahr, dass wichtige Daten gestohlen, manipuliert, verschlüsselt oder vernichtet werden. Ebenso können aber auch Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden. Dieser Aspekt wird durch die Tatsache begünstigt, dass ein Datenaustausch im Ausland häufig über unsichere Medien stattfindet. Dieser wichtige Aspekt ist den Mitarbeitenden jedoch nicht immer bewusst.

## 2.3. Vortäuschen einer falschen Identität

Im Rahmen von Kommunikation auf Reisen besteht eine erhöhte Gefahr, dass bei Angriffen sowohl persönlich als auch elektronisch versucht wird, eine falsche Identität vorzutäuschen oder eine autorisierte Identität zu übernehmen, z. B. durch Maskerade, Spoofing-Arten, Hijacking oder Man-in-the-Middle-Angriffe. Hierbei können Benutzende über die Identität ihres Kommunikationspartners oder ihrer Kommunikationspartnerin so getäuscht werden, dass sie schützenswerte Informationen preisgeben. Eine falsche digitale Identität erlangt die angreifende Person z. B. durch das Ausspähen von Benutzenden-ID und Passwort, die Manipulation des Absenderfeldes einer Nachricht oder durch die Manipulation einer Adresse im Netz.

Mitarbeitende kennen bei ausländischen Geschäftsbeziehungen ihre Kontaktpersonen nicht immer persönlich. Daher kann es passieren, dass sich fremde Personen mit dem Namen der Kontaktpersonen vorstellen und die Mitarbeitenden ihnen vertrauen und wertvolle Informationen weitergeben.

Die Sicherheitsanforderungen an Vertraulichkeit und Integrität können in institutionsfremden, vor allem ausländischen Gebäuden und Räumen, nie vollständig erfüllt werden. Daher besteht immer ein Restrisiko, dass auch Geräte manipuliert sein könnten, die normalerweise als sicher eingestuft würden. Dazu gehört etwa die Rufnummernanzeige am Telefon oder die Faxkennung eines Faxabsenders, durch die eine falsche Identität vorgetäuscht und Informationen erlangt werden können.

## 2.4. Fehlendes Sicherheitsbewusstsein und Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass es in Institutionen zwar organisatorische Regelungen und technische Sicherheitsverfahren für tragbare IT-Systeme und mobile Datenträger gibt, diese jedoch von den Beschäftigten nicht ausreichend beachtet und umgesetzt werden. Zum Beispiel lassen Mitarbeitende mobile Datenträger oft unbeaufsichtigt im Besprechungsraum oder auch im Zugabteil zurück.

Darüber hinaus werden Geschenke in Form von Datenträgern, wie etwa USB-Sticks, von Mitarbeitenden angenommen und unüberlegt an das eigene Notebook angeschlossen. Hier besteht dann die Gefahr, dass das Notebook mit Schadsoftware infiziert wird und dadurch schützenswerte Daten gestohlen, manipuliert oder verschlüsselt werden.

In öffentlichen Verkehrsmitteln oder auch während Geschäftsessen ist zudem immer wieder zu beobachten, dass Menschen offene Gespräche über geschäftskritische Informationen führen. Diese können dann von Außenstehenden leicht mitgehört und möglicherweise zum schwerwiegenden Nachteil der Mitarbeitenden oder ihrer Institution verwendet werden.

## 2.5. Verstoß gegen lokale Gesetze oder Regelungen

Bei Reisen ins Ausland sind insbesondere abweichende Gesetze und Regularien der Zieldestination zu berücksichtigen, da sich diese massiv von der nationalen Rechtslage unterscheiden können.

Einschlägige Gesetze und Verordnungen des Ziellandes, z. B. zu Datenschutz, Informationspflichten, Haftung oder Informationszugriffe für Dritte, sind Reisenden häufig unbekannt oder werden falsch eingeschätzt. Dadurch kann nicht nur im Ausland, sondern auch im Inland gegen eine Vielzahl von Gesetzen verstoßen werden, beispielsweise wenn im Ausland personenbezogene Daten inländischer Kundschaft bei einer Auslandsdienstreise ungeschützt über öffentliche Netze übertragen werden.

## 2.6. Nötigung, Erpressung, Entführung und Korruption

Im Ausland gelten oft andere Sicherheitsrisiken aufgrund politischer und gesellschaftlicher Umstände. Die Sicherheit von Informationen, aber auch die Sicherheit der Reisenden selbst, könnte bei Auslandsreisen etwa durch Nötigung, Erpressung oder Entführung gefährdet werden. Mitarbeitende könnte zum Beispiel Gewalt angedroht werden, um sie zur Herausgabe von schützenswerten Daten zu

zwingen. Dabei werden sie dann genötigt, Sicherheitsrichtlinien und -maßnahmen zu umgehen bzw. zu missachten. Im Fokus stehen hierbei oftmals hochrangige Führungskräfte oder Mitarbeitende, die eine besondere Vertrauensstellung genießen.

Angriffe verfolgen vor allem das Ziel, schützenswerte Informationen zu stehlen oder zu manipulieren, um den Ablauf der Geschäftsprozesse zu beeinträchtigen oder sich und andere zu bereichern. Hier spielen vor allem politische, ideologische und wirtschaftliche Ziele der Angreifenden eine Rolle.

Neben der Androhung von Gewalt besteht auch die Möglichkeit der Bestechung oder Korruption. Reisenden werden etwa gezielt Geld oder andere Vorteile angeboten, um sie zur Herausgabe von vertraulichen Informationen an Unbefugte bzw. zu Sicherheitsverletzungen zu bewegen.

Generell werden durch Nötigung, Erpressung, Entführung und Korruption die Regelungen zur Informationssicherheit gestört bzw. ausgehebelt.

## 2.7. Informationen aus unzuverlässiger Quelle

Im Rahmen einer Auslandstätigkeit können den Reisenden absichtlich falsche oder irreführende Informationen zugespielt werden, um sie zu täuschen. In Folge dieser Täuschung könnten falsche Aussagen in geschäftskritische Berichte einfließen. Dies kann unter anderem dazu führen, dass geschäftsrelevante Informationen auf einer falschen Datenbasis beruhen, Berechnungen falsche Ergebnisse liefern und darauf basierend falsche Entscheidungen getroffen werden.

## 2.8. Diebstahl oder Verlust von Geräten, Datenträgern und Dokumenten

Insbesondere auf Reisen im Ausland ist damit zu rechnen, dass mobile Endgeräte leicht verloren gehen oder gestohlen werden. Je kleiner und begehrter diese Geräte sind, desto höher ist dieses Risiko. Neben dem rein materiellen Schaden durch den unmittelbaren Verlust des mobilen Gerätes kann durch die Offenlegung schützenswerter Daten, z. B. E-Mails, Notizen von Besprechungen oder Adressen, weiterer finanzieller Schaden entstehen. Außerdem kann der Ruf der Institution geschädigt werden.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins *CON.7 Informationssicherheit auf Auslandsreisen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Benutzende, IT-Betrieb, Personalabteilung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### 3.1. Basis-Anforderung

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

## **CON.7.A1 Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen (B)**

Alle für die Informationssicherheit relevanten Aspekte, die in Verbindung mit den Tätigkeiten im Ausland stehen, MÜSSEN betrachtet und geregelt werden. Die Sicherheitsmaßnahmen, die in diesem Zusammenhang ergriffen werden, MÜSSEN in einer Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen dokumentiert werden. Diese Sicherheitsrichtlinie oder ein entsprechendes Merkblatt mit zu beachtenden Sicherheitsmaßnahmen MÜSSEN transnational agierenden Mitarbeitenden ausgehändigt werden.

Erweiternd MUSS ein Sicherheitskonzept zum Umgang mit tragbaren IT-Systemen auf Auslandsreisen erstellt werden, das alle Sicherheitsanforderungen und -maßnahmen angemessen detailliert beschreibt. Die Umsetzung des Sicherheitskonzeptes MUSS regelmäßig überprüft werden.

## **CON.7.A2 Sensibilisierung der Mitarbeitenden zur Informationssicherheit auf Auslandsreisen (B)**

Benutzende MÜSSEN im verantwortungsvollen Umgang mit Informationstechnik bzw. tragbaren IT-Systemen auf Auslandsreisen sensibilisiert und geschult werden. Benutzende MÜSSEN die Gefahren kennen, die durch den unangemessenen Umgang mit Informationen, die unsachgemäße Vernichtung von Daten und Datenträgern oder durch Schadsoftware und den unsicheren Datenaustausch entstehen können. Außerdem MÜSSEN die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgezeigt werden. Die Benutzenden MÜSSEN dazu befähigt und darin bestärkt werden, einem Verlust oder Diebstahl vorzubeugen bzw. bei Ungereimtheiten fachliche Beratung einzuholen. Außerdem SOLLTEN Mitarbeitende auf gesetzliche Anforderungen einzelner Reiseziele in Bezug auf die Reisesicherheit hingewiesen werden. Hierzu MUSS sich der oder die Informationssicherheitsbeauftragte über die gesetzlichen Anforderungen im Rahmen der Informationssicherheit (z. B. Datenschutz, IT-Sicherheitsgesetz) informieren und die Mitarbeitenden sensibilisieren.

## **CON.7.A3 Identifikation länderspezifischer Regelungen, Reise- und Umgebungsbedingungen (B) [Personalabteilung]**

Vor Reiseantritt MÜSSEN die jeweils geltenden Regelungen der einzelnen Länder durch das Informationssicherheitsmanagement bzw. die Personalabteilung geprüft und an die entsprechenden Mitarbeitenden kommuniziert werden.

Die Institution MUSS geeignete Regelungen und Maßnahmen erstellen, umsetzen und kommunizieren, die den angemessenen Schutz interner Daten ermöglichen. Dabei MÜSSEN die individuellen Reise- und Umgebungsbedingungen berücksichtigt werden.

Außerdem MÜSSEN sich Mitarbeitende vor Reiseantritt mit den klimatischen Bedingungen des Reiseziels auseinandersetzen und abklären, welche Schutzmaßnahmen er für sich benötigt, z. B. Impfungen, und welche Schutzmaßnahmen für die mitgeführte Informationstechnik nötig sind.

## **CON.7.A4 Verwendung von Sichtschutz-Folien (B) [Benutzende]**

Benutzende MÜSSEN insbesondere im Ausland darauf achten, dass bei der Arbeit mit mobilen IT-Geräten keine schützenswerten Informationen ausgespäht werden können. Dazu MUSS ein angemessener Sichtschutz verwendet werden, der den gesamten Bildschirm des jeweiligen Gerätes umfasst und ein Ausspähen von Informationen erschwert.

## **CON.7.A5 Verwendung der Bildschirm-/Code-Sperre (B) [Benutzende]**

Eine Bildschirm- bzw. Code-Sperre, die verhindert, dass Dritte auf die Daten mobiler Endgeräte zugreifen können, MUSS verwendet werden. Die Benutzenden MÜSSEN dazu einen angemessenen Code bzw. ein sicheres Gerätepasswort verwenden. Die Bildschirmsperre MUSS sich nach einer kurzen Zeit der Inaktivität automatisch aktivieren.

### **CON.7.A6 Zeitnahe Verlustmeldung (B) [Benutzende]**

Mitarbeitende MÜSSEN ihrer Institution umgehend melden, wenn Informationen, IT-Systeme oder Datenträger verloren gegangen sind oder gestohlen wurden. Hierfür MUSS es klare Meldewege und Kontaktpersonen innerhalb der Institution geben. Die Institution MUSS die möglichen Auswirkungen des Verlustes bewerten und geeignete Gegenmaßnahmen ergreifen.

### **CON.7.A7 Sicherer Remote-Zugriff auf das Netz der Institution (B) [IT-Betrieb, Benutzende]**

Um Beschäftigten auf Auslandsreisen einen sicheren Fernzugriff auf das Netz der Institution zu ermöglichen, MUSS zuvor vom IT-Betrieb ein sicherer Remote-Zugang eingerichtet worden sein, z. B. ein Virtual Private Network (VPN). Der VPN-Zugang MUSS kryptografisch abgesichert sein. Außerdem MÜSSEN Benutzende über angemessen sichere Zugangsdaten verfügen, um sich gegenüber dem Endgerät und dem Netz der Institution erfolgreich zu authentisieren. Mitarbeitende MÜSSEN den sicheren Remote-Zugriff für jegliche darüber mögliche Kommunikation nutzen. Es MUSS sichergestellt werden, dass nur autorisierte Personen auf IT-Systeme zugreifen dürfen, die über einen Fernzugriff verfügen. Mobile IT-Systeme MÜSSEN im Rahmen der Möglichkeiten vor dem direkten Anschluss an das Internet durch eine restriktiv konfigurierte Personal Firewall geschützt werden.

### **CON.7.A8 Sichere Nutzung von öffentlichen WLANs (B) [Benutzende]**

Grundsätzlich MUSS geregelt werden, ob mobile IT-Systeme direkt auf das Internet zugreifen dürfen.

Für den Zugriff auf das Netz der Institution über öffentlich zugängliche WLANs MÜSSEN Benutzende ein VPN oder vergleichbare Sicherheitsmechanismen verwenden (siehe CON.7.A7 *Sicherer Remote-Zugriff* und NET.2.2 *WLAN-Nutzung*). Bei der Benutzung von WLAN-Hotspots MÜSSEN ebenfalls Sicherheitsmaßnahmen getroffen werden, siehe auch INF.9 *Mobiler Arbeitsplatz*.

### **CON.7.A9 Sicherer Umgang mit mobilen Datenträgern (B) [Benutzende]**

Werden mobile Datenträger verwendet, MÜSSEN Benutzende vorab gewährleisten, dass diese nicht mit Schadsoftware infiziert sind. Vor der Weitergabe mobiler Datenträger MÜSSEN Benutzende außerdem sicherstellen, dass keine schützenswerten Informationen darauf enthalten sind. Wird er nicht mehr genutzt, MUSS der Datenträger sicher gelöscht werden, insbesondere wenn er an andere Personen weitergegeben wird. Dazu MUSS der Datenträger mit einem in der Institution festgelegten, ausreichend sicheren Verfahren überschrieben werden.

### **CON.7.A10 Verschlüsselung tragbarer IT-Systeme und Datenträger (B) [Benutzende, IT-Betrieb]**

Damit schützenswerte Informationen nicht durch unberechtigte Dritte eingesehen werden können, MÜSSEN Mitarbeitende vor Reiseantritt sicherstellen, dass alle schützenswerten Informationen entsprechend den internen Richtlinien abgesichert sind. Mobile Datenträger und IT-Systeme SOLLTEN dabei vor Reiseantritt durch Benutzende oder den IT-Betrieb verschlüsselt werden. Die kryptografischen Schlüssel MÜSSEN getrennt vom verschlüsselten Gerät aufbewahrt werden. Bei der Verschlüsselung von Daten SOLLTEN die gesetzlichen Regelungen des Ziellandes beachtet werden. Insbesondere landesspezifische Gesetze zur Herausgabe von Passwörtern und zur Entschlüsselung von Daten SOLLTEN berücksichtigt werden.

### **CON.7.A12 Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten (B) [Benutzende]**

Die Institution MUSS den Beschäftigten Möglichkeiten aufzeigen, schutzbedürftige Dokumente angemessen und sicher zu vernichten. Benutzende MÜSSEN diese Regelungen einhalten. Sie DÜRFEN interne Unterlagen der Institution NICHT entsorgen, bevor diese sicher vernichtet worden sind. Ist dies vor Ort nicht möglich oder handelt es sich um Dokumente bzw. Datenträger mit besonders schützenswerten Informationen, MÜSSEN diese bis zur Rückkehr behalten und anschließend angemessen vernichtet werden.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

### CON.7.A11 Einsatz von Diebstahl-Sicherungen (S) [Benutzende]

Zum Schutz der mobilen IT-Systeme außerhalb der Institution SOLLTEN Benutzende Diebstahl-Sicherungen einsetzen, vor allem dort, wo ein erhöhter Publikumsverkehr herrscht oder die Fluktuation von Benutzenden sehr hoch ist. Die Beschaffungs- und Einsatzkriterien für Diebstahl-Sicherungen SOLLTEN an die Prozesse der Institution angepasst und dokumentiert werden.

### CON.7.A13 Mitnahme notwendiger Daten und Datenträger (S) [Benutzende]

Vor Reiseantritt SOLLTEN Benutzende prüfen, welche Daten während der Reise nicht unbedingt auf den IT-Systemen gebraucht werden. Ist es nicht notwendig, diese Daten auf den Geräten zu lassen, SOLLTEN diese sicher gelöscht werden. Ist es nötig, schützenswerte Daten mit auf Reisen zu nehmen, SOLLTE dies nur in verschlüsselter Form erfolgen. Darüber hinaus SOLLTE schriftlich geregelt sein, welche mobilen Datenträger auf Auslandsreisen mitgenommen werden dürfen und welche Sicherheitsmaßnahmen dabei zu berücksichtigen sind (z. B. Schutz vor Schadsoftware, Verschlüsselung geschäftskritischer Daten, Aufbewahrung mobiler Datenträger). Die Mitarbeitenden SOLLTEN diese Regelungen vor Reiseantritt kennen und beachten.

Diese sicherheitstechnischen Anforderungen SOLLTEN sich nach dem Schutzbedarf der zu bearbeitenden Daten im Ausland und der Daten, auf die zugegriffen werden soll, richten.

### CON.7.A14 Kryptografisch abgesicherte E-Mail-Kommunikation (S) [Benutzende, IT-Betrieb]

Die E-Mail-basierte Kommunikation SOLLTEN Benutzende entsprechend den internen Vorgaben der Institution kryptografisch absichern. Die E-Mails SOLLTEN ebenfalls geeignet verschlüsselt bzw. digital signiert werden. Öffentliche IT-Systeme, etwa in Hotels oder Internetcafés, SOLLTEN NICHT für den Zugriff auf E-Mails genutzt werden.

Bei der Kommunikation über E-Mail-Dienste, z. B. Webmail, SOLLTE durch den IT-Betrieb vorab geklärt werden, welche Sicherheitsmechanismen beim Provider umgesetzt werden und ob damit die internen Sicherheitsanforderungen erfüllt werden. Hierzu SOLLTE z. B. der sichere Betrieb der Server, der Aufbau einer verschlüsselten Verbindung und die Dauer der Datenspeicherung zählen.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

### CON.7.A15 Abstrahlsicherheit tragbarer IT-Systeme (H)

Es SOLLTE vor Beginn der Reise festgelegt werden, welchen Schutzbedarf die einzelnen Informationen haben, die auf dem mobilen Datenträger bzw. Client der Mitarbeitenden im Ausland verarbeitet werden. Die Institution SOLLTE prüfen, ob die mitgeführten Informationen einen besonderen Schutzbedarf haben, und entsprechend abstrahlarme bzw. -sichere Datenträger und Clients einsetzen.

### CON.7.A16 Integritätsschutz durch Check-Summen oder digitale Signaturen (H) [Benutzende]

Benutzende SOLLTEN Check-Summen im Rahmen der Datenübertragung und Datensicherung verwenden, um die Integrität der Daten überprüfen zu können. Besser noch SOLLTEN digitale Signaturen verwendet werden, um die Integrität von schützenswerten Informationen zu bewahren.



### **CON.7.A17 Verwendung vorkonfigurierter Reise-Hardware (H) [IT-Betrieb]**

Damit schützenswerte Informationen der Institution auf Auslandsreisen nicht von Dritten abgegriffen werden können, SOLLTE der IT-Betrieb den Mitarbeitenden vorkonfigurierte Reise-Hardware zur Verfügung stellen. Diese Reise-Hardware SOLLTE auf Basis des Minimalprinzips nur die Funktionen und Informationen bereitstellen, die zur Durchführung der Geschäftstätigkeit unbedingt erforderlich sind.

### **CON.7.A18 Eingeschränkte Berechtigungen auf Auslandsreisen (H) [IT-Betrieb]**

Vor Reiseantritt SOLLTE geprüft werden, welche Berechtigungen Mitarbeitende wirklich brauchen, um ihrem Alltagsgeschäft im Ausland nachgehen zu können. Dabei SOLLTE geprüft werden, ob Zugriffsrechte für die Reisedauer der Benutzenden durch den IT-Betrieb entzogen werden können, um einen unbefugten Zugriff auf Informationen der Institution zu verhindern.

## **4. Weiterführende Informationen**

### **4.1. Wissenswertes**

Die „Initiative Wirtschaftsschutz“ gibt auf ihrer Website unter <https://www.wirtschaftsschutz.info> weiterführende Informationen zur Sicherheit auf Geschäftsreisen.