A09 Checkliste Organisatorische Anforderungen

Die Technische Maßnahmen allein genügen nicht, nur durch die permanente Umsetzung und Einhaltung von organisatorischen Regeln ist ein sicherer Betrieb möglich. Nachfolgende Checkliste gibt Ihnen einen Überblick über unsere Anforderungen.

Tipp: Analog zur Checkliste der Befehlsstelle und der Checkliste IT-Systemsicherheit senden Sie bitte das ausgefüllte Dokument an uns zurück. Aus diesem sollte hervorgehen, welche organisatorischen Anforderungen von Ihnen umgesetzt werden.

Umsetzung von organisatorischen Regeln in ortsfesten Befehlsstellen

P/E	Anforderung	Umgesetzt? (Ja/Nein)
P	**Geschlossene Fenster und Türen** Fenster und von außen zugängliche Türen, etwa von Balkonen oder Terrassen, MÜSSEN zu Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Räume MÜSSEN verschlossen werden, falls dort vertrauliche Informationen zurückgelassen werden. Dafür MUSS es eine entsprechende Anweisung geben. Alle Zutrittsberechtigten SOLLTEN dazu verpflichtet werden, der Anweisung nachzukommen. Es MUSS regelmäßig überprüft werden, ob die Fenster und Innen- sowie Außentüren nach Verlassen des Gebäudes verschlossen sind. Brand- und Rauchschutztüren DÜRFEN NUR dann dauerhaft offen gehalten werden, wenn dies durch zugelassene Feststellanlagen erfolgt [INF7.A2].	
P	**Frei zugängliche Zugangsdaten vermeiden** Zugangsdaten, also Benutzernamen und Passwörter dürfen nicht aufgeschrieben und für jedermann ersichtlich und zugänglich sein.	
E	**Aufgeräumter Arbeitsplatz** Die zutrittsberechtigten Personen sollten dazu motiviert werden, die Arbeitsplätze aufgeräumt zu hinterlassen, um unbefugten Personen keinen Zugang zu IT-Anwendungen zu ermöglichen und den Zugriff auf vertrauliche Informationen, z.B. ausgedruckte Einsatzunterlagen auszuschließen [INF7.A6; INF7.A7].	

Umsetzung von organisatorischen Regeln in mobilen Befehlsstellen

P/E	Anforderung	Umgesetzt? (Ja/Nein)
P	**Wartung, Inspektion und Updates** Fahrzeuge, die als mobile Befehlsstelle eingesetzt und die dazugehörenden IT-Komponenten MÜSSEN nach den Vorgaben des Herstellers gewartet werden. Hierbei MUSS beachtet werden, dass die Intervalle der herkömmlichen Wartung des Fahrzeugs und von Updates der integrierten IT-Komponenten voneinander abweichen können. Es MUSS daher klar geregelt werden, wer in welcher Umgebung die Updates installieren darf. Wartungs- und Reparaturarbeiten MÜSSEN von befugtem und qualifiziertem Personal in einer sicheren Umgebung durchgeführt werden. Dabei SOLLTE schon vor der Wartung geklärt werden, wie mit Fremdfirmen umgegangen wird. Werden Fahrzeuge in fremden Einrichtungen gewartet, SOLLTE geprüft werden, ob alle nicht benötigten, zum Fahrzeug dazugehörigen portablen IT-Systeme vorab entfernt werden.	

	Werden die Fahrzeuge wieder in den Einsatzbetrieb integriert, MUSS mittels Checkliste geprüft werden, ob alle Beanstandungen und Mängel auch behoben wurden. Es MUSS auch geprüft werden, ob die vorhandenen IT-Komponenten einsatzfähig sind [INF11.A2].	
P	**Abgeschlossene Türen und Fenster** Personen haben bei Abwesenheit die Befehlsstelle abzuschließen. Alternativ ist der Zugang und Zugriff auf die IuK-Technik, Einsatzunterlagen und der personenbezogenen Daten, z.B. in Einsatzberichten und –protokollen für unberechtigte Personen zu unterbinden [INF7.A2].	
P	**Frei zugängliche Zugangsdaten vermeiden** Für alle Tätigkeiten, die sich auf die Sicherheit der in den mobilen Befehlsstellen verarbeiteten Informationen auswirken können, MUSS festgelegt werden, welche Schutzvorkehrungen dabei zu treffen sind. Dies MUSS für jede Art von Information gelten, auch für Gespräche in den mobilen Befehlsstellen. Es MUSS geklärt werden, unter welchen Rahmenbedingungen Personen auf welche Art von Informationen zugreifen dürfen. Außerdem MUSS geregelt werden, in welchem Umfang Infotainmentsysteme, Anwendungen und sonstige Services der Fahrzeuge genutzt werden dürfen. Des Weiteren MUSS festgelegt werden, wie Schnittstellen abzusichern sind. In Dienstanweisungen MUSS geregelt werden, wie mitgeführte IT in den Fahrzeugen verwendet und aufbewahrt werden darf [INF7.A6, INF7.A7, INF11.A3].	
E	**Aufgeräumter Arbeitsplatz** Die zutrittsberechtigten Personen sollten dazu motiviert werden, die Arbeitsplätze aufgeräumt zu hinterlassen, um unbefugten Personen keinen Zugang zu IT-Anwendungen zu ermöglichen und den Zugriff auf vertrauliche Informationen, z.B. ausgedruckte Einsatzunterlagen auszuschließen [INF7.A6; INF7.A7].	
E	**Sicherstellung der Versorgung** Bevor Fahrzeuge, als mobile Befehlsstelle eingesetzt werden, SOLLTE geplant werden, wie diese mit Betriebsstoffen während des Einsatzes versorgt werden. Die Fahrzeuge SOLLTEN dabei während des Einsatzes immer ausreichend mit Betriebsstoffen versorgt werden [INF11.A9].	
E	**Festlegung von Handlungsanweisungen** Für alle wesentlichen Situationen im Einsatzgeschehen SOLLTEN Handlungsanweisungen in Form von Checklisten vorliegen. Hierbei SOLLTE auch der Fall berücksichtigt werden, dass das Fahrzeug selbst gestohlen wird. Die Handlungsanweisungen SOLLTEN insbesondere nachfolgende Szenarien behandeln: • Ausfall von IT-Komponenten, • Notfallsituationen wie Unfälle, • unerlaubtes Betreten der Fahrzeuge sowie • Diebstahl der Fahrzeuge oder darin abgelegter Gegenstände mit Relevanz für die Informationssicherheit. Die Zuständigkeiten für die einzelnen Aufgaben SOLLTEN in der Checkliste dokumentiert sein. Die Anweisungen SOLLTEN von den Fahrzeugnutzern in den entsprechenden Situationen angewendet werden. Anhand der Checkliste SOLLTE dokumentiert werden, wie sie in diesen Situationen vorgegangen sind [INF11.A6]. **Hinweis:** Für den Fall, dass Fahrzeuge als mobile Befehlsstelle ausfallen, SOLLTEN vorbereitende Maßnahmen getroffen werden [INF11.A11].	
	Sachgerechter Umgang mit mobilen Befehlsstellen und schützenswerten Informationen Der Aufgabenträger SOLLTE die Handlungsanweisungen zur Benutzung der mobilen Befehlsstelle um Aspekte ergänzen, wann, wie und wo die mobile Befehlsstelle sachgerecht	

	abgestellt bzw. angedockt werden dürfen. Hierbei SOLLTE primär die Frage beantwortet werden, welche Umgebungen die mobile Befehlsstelle angemessen vor unerlaubten Zutritt oder Sachbeschädigung schützen. Des Weiteren SOLLTE hierbei berücksichtigt werden, welche Informationen und IT-Systeme in der mobilen Befehlsstelle aufbewahrt werden dürfen. Ausreichende Maßnahmen zum Zutrittsschutz SOLLTEN ergriffen werden. Die Ladung der mobilen Befehlsstelle SOLLTE sicher verstaut werden. Es SOLLTE sichergestellt werden, dass schützenswerte Informationen nicht von außerhalb der Befehlsstelle von Unbefugten eingesehen, mitgehört oder entwendet werden können. Das Führungspersonal SOLLTE mit der grundlegenden Funktionsweise der Befehlsstelle und den betreffenden IT-Komponenten vertraut gemacht werden. Das Führungspersonal SOLLTE auch über die bestehenden Sicherheitsrisiken informiert werden [INF11.A7].	

Entsorgung

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Geregelte Außerbetriebnahme von Hardware in der Befehlsstelle** Bei der Außerbetriebnahme von Komponenten in der Befehlsstelle z.B. Computer, Drucker, Netzwerkroutern, Datensicherungsplatten usw. sollte sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen und dass keine sensitiven Daten zurückbleiben. Insbesondere bei einer Weiterverwendung der Komponenten ist sicherzustellen, dass die gespeicherten Daten vorab gelöscht werden. Werden Fahrzeuge ausgesondert, SOLLTEN keine schützenswerten Informationen in den Fahrzeugen verbleiben. Bevor Fahrzeuge endgültig ausgesondert werden, SOLLTE anhand der Inventarliste geprüft werden, ob keine inventarisierte Gegenstände und darüber hinaus relevante Gegenstände zurückgelassen worden sind [INF11.A10].	

Verlustmeldungen / Diebstahl

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Verlustmeldung** Der Verlust von Informationstechnik ist nicht schön, kommt aber vor, z.B. durch Diebstahl oder ein Notebook / Laptop geht verloren. Zum Schutz der Zugangssicherheit müssen in der IRLS Lausitz Sicherheitsmaßnahmen ergriffen werden. Aus diesem Grund muss umgehend gemeldet werden, wenn z.B. ein Laptop verloren gegangen ist oder gestohlen wurde. Melden Sie den Verlust über die IRLS Lausitz. Wenn verlorene Laptops wieder auftauchen, sind diese komplett neu zu installieren [SYS2.1.A.28; SYS3.1.A12].	

Umzug / Auszug

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
E	**Umzug / Auszug**	

	Steht ein Umzug in ein anderes Befehlsstellenobjekt oder ein Auszug bevor, empfehlen wir, ein Bestandsverzeichnis aller für die Befehlsstelle relevanten Dinge (Hardware, Software, Telefon, Drucker Datenträger, Unterlagen etc.) zu erstellen. Vor dem Umzug ist die Möglichkeit der Einsatzbereitschaft der Befehlsstelle zu klären und der IRLS Lausitz mitzuteilen. Nach dem Auszug sollten alle Räume nach zurückgelassenen Dinge überprüft werden.	

Notfallmanagement

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
E	**Notfallmanagement** Existiert ein Konzept, z.B. ein Notfallhandbuch, in welchem Maßnahmen im Umgang mit Notfällen / Unterbrechungen der Führungsaufgabe und dem Wiederanlauf geregelt sind?	