A06 CHECKLISTE IT-SYSTEM

Die Checkliste IT-System erfordert ein gewisses technisches Grundverständnis für Computer- und Betriebssysteme.

Computersysteme in ortsfesten Befehlsstellen (Windows 10 Professional)

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Sichere Installation und Konfiguration** Nur für die Aufgabenwahrnehmung notwendige Komponenten und Programme sollten auf dem Windows 10-Computersystem installiert werden. Dadurch lassen sich mögliche Ursachen für Computerfehler reduzieren und ungewollte Datenübertragungen an Microsoft und anderen Drittanbieter werden ausgeschlossen. Die Installation und Konfiguration der IT-Systeme sollte von Personen mit Computerkenntnissen (Administratoren vor Ort) durchgeführt werden [SYS2.1.A15; SYS2.1.A16, SYS2.2.3.A4; SYS2.2.3.A13; SYS2.2.3.A14; SYS2.2.3.A15; SYS2.2.3.A16]. **Tipp:** Windows 10 verfügt über eine Werkseinstellungsfunktion, diese sollte zu Beginn ausgeführt werden. Bei der nachfolgenden Erstanmeldung sind sämtliche angebotenen Telemetriedaten, Cloud- & Online-Dienste, die SmartScreen-Funktion, der Sprachassistent Cortana, Synchronisationsmechanismen, wie z.B. OneDrive und die Anbindung an den Windows Store zu deaktivieren. Anschließend sollten Sie vorinstallierte Demo-Versionen, Virenschutzprogramme und Computerspiele deinstallieren. Bei späteren Anpassungen des Computersystems sollten Sie stets über ein funktionsfähiges Backup verfügen, um das vorherige Systemabbild im Bedarfsfall schneller wiederherzustellen. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Keine Netzkopplung** Die Kopplung zwischen dem Befehlsstellennetz und anderen Netzwerken, z.B. dem internen Netzwerk, dem Internet und anderen Netzen ist nicht zulässig. Unter einer Netzkopplung wird auch das zeitweilige Einbinden des Computersystems der Befehlsstelle in ein anderes Netzwerk verstanden. Eine Nicht-Beachtung stellt eine zusätzliche Gefährdung für die Verfügbarkeit, Integrität und Vertraulichkeit des gesamten Befehlsstellennetzes sowie der IRLS Lausitz dar, da z.B. somit die Möglichkeit besteht, Schadcode in das geschlossene Netzwerk zu übertragen [SYS3.1.A8]. **Eine Nichtbeachtung führt zur Sperrung des Netzzugangs.**	☐

P	**Aktualisierung des Betriebssystems** Das Betriebssystem ist regelmäßig mit Sicherheitspatches und Updates zu aktualisieren. Der Client ist so einzurichten, dass automatisch Patches & Updates heruntergeladen und installiert werden [SYS2.1.A3; SYS2.1.A14]. **Hinweis:** Um die Sicherheitspatches und Updates für das Betriebssystem im geschlossenen Netzwerk zu erhalten, stellt die IRLS Lausitz einen Update-Dienst zentral bereit. Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Rollentrennung** Das Computersystem ist so einzurichten, dass die typische Nutzung als Befehlsstelle nicht mit Administrationsrechten erfolgt. Nur Administratoren dürfen Administrationsrechte erhalten, um die Systemkonfiguration zu ändern, Anwendungen zu installieren und zu entfernen [SYS2.1.A2; SYS2.1.A13]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Anbindung an zentralen Zeitgeber (NTP-Server)** Der Befehlsstellenclient ist an den zentralen Zeitserver der IRLS Lausitz anzubinden. Damit wird die Datenintegrität sichergestellt und Widersprüche vermieden, indem die identische Zeit in der Befehlsstelle bereitsteht. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Einsatz eines Virenschutzprogramm** Auf dem Befehlsstellencomputer ist ein Virenschutzprogramm einzusetzen. Die IRLS Lausitz stellt zentral ein Virenschutzprogramm zur Verfügung und liefert regelmäßig Updates [SYS2.1.A6; SYS2.2.3.A5]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Fernwartung** Im Störungsfall ist eine schnelle Unterstützung von großem Vorteil. Zu diesem Zweck ist die Einrichtung einer Fernwartungsanwendung erforderlich, diese ist am Befehlsstellenclient durch den Administrator vor Ort zu installieren und zu konfigurieren (Siehe Punkt 7.2.4 Betriebshandbuch).	☐

	Hinweis: Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	
P	**Systemüberwachung** Der Befehlsstellenclient ist in das Monitoring-System der IRLS Lausitz einzubinden. Darüber werden der Systemzustand und die Funktionsfähigkeit des Clients laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an das administrative Personal vor Ort gemeldet. In der Folge werden Störungsquellen, Gefährdungen rechtzeitig erkannt und behoben. Dadurch erhöht sich die Betriebssicherheit des Befehlsstellenclients [SYS2.1.A29; SYS2.1.A41]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
E	**Benutzerauthentisierung** Der Zugang zu den durch die IRLS Lausitz bereitgestellten Anwendungen wird durch separate Zugangsdaten geschützt. Die Benutzerauthentisierung am Betriebssystem (z.B. durch Abfrage von Benutzername und Passwort) ist dennoch empfehlenswert, insbesondere wenn vertrauliche Informationen auf dem Computersystem gespeichert werden [SYS2.1.A1; SYS2.2.3.A17].	☐
E	**Regelmäßige Datensicherung** Es gibt unterschiedliche Gründe für Datenverluste, häufig sind defekte Festplatten oder Computerviren ein Grund. Sofern ein Datenverlust eingetreten ist, ist die Rettung eine Datensicherung. Empfehlenswert ist daher die regelmäßige Datensicherung des Computersystems, um schnell wieder betriebsfähig zu sein. Dabei sollte die Sicherungskopie nicht aktiv mit dem Computersystem verbunden sein (Offline-Sicherung). Ferner sollten Sie regelmäßig testen, ob eine Datenwiederherstellung möglich ist [SYS2.1.A4]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz. Die Sicherungskopien enthalten eine vollständige Kopie des Computersystems und sollten dementsprechend sicher verwahrt und vor unberechtigten Zugriff geschützt werden.	☐
E	**Bildschirmsperre** Nicht immer ist es erforderlich, dass ein aktiver Befehlsstellencomputer genutzt wird. Dadurch besteht für unberechtigte Personen die Möglichkeit, Zugriff auf die vertraulichen Einsatzdaten zu gelangen. Empfehlenswert ist die Einrichtung einer Bildschirmsperre, die nach einer gewissen Zeit automatisiert den Computerzugriff sperrt und zur Reaktivierung eine Benutzerauthentifizierung verlangt [SYS2.1.A5].	☐

	Hinweis: Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	
E	**Absicherung des Boot-Vorgangs** Der Startvorgang des Computersystems, dass sogenannte "Booten" muss gegen Manipulationen abgesichert werden. Dafür muss vom Administrator vor Ort festgelegt werden, von welchen Medien gebootet werden darf. Es ist sicherzustellen, dass nur Administratoren die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können [SYS2.1.A8; SYS2.1.A36]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
E	**Datei- und Freigabeberechtigungen** Der Zugriff auf Dateien und Ordner auf dem lokalen System sowie auf Netzwerkfreigaben ist so gering wie möglich zu halten. Sie sollten die Speicherung von vertraulichen Daten in Freigabeordnern vermeiden [SYS.2.2.3.A12]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
E	**Umgang mit Wechseldatenträgern** Über Wechseldatenträger, z.B. USB-Sticks, Speicherkarten, CDs, DVDs usw. kann Schadcode auf das Computersystem gelangen und es können vertrauliche Daten kopiert und unberechtigt entwendet werden. Um diese Gefährdungen auszuschließen, ist die Einschränkung der Nutzung von Wechseldatenträgern empfehlenswert [SYS2.1.A24] **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
E	**Verschlüsselung des Computersystems** Wenn vertrauliche Informationen auf dem Computersystem gespeichert werden, z.B. Einsatzberichte als PDF-Datei o.ä., sollten die schutzbedürftigen Dateien, ausgewählte Dateisystembereiche oder besser die gesamte Festplatte verschlüsselt werden [SYS2.1.A28, SYS2.2.3.A21]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐

E	**Personal-Firewall** Auf dem Betriebssystem des Befehlsstellenclients sollte die Personal Firewall aktiv sein. Die Filterregeln der Firewall sollten so restriktiv wie möglich sein. Sie sind regelmäßig zu testen. Die Personal Firewall ist so zu konfigurieren, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können [SYS 2.1.A31]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
E	**Windows PowerShell** Die Ausführung der PowerShell sowie von WPS-Dateien sollte nur für Administratoren vor Ort erlaubt sein [SYS2.2.3.A24]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
E	**Unterbrechungsfreie Stromversorgung** Der Befehlsstellenclient sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Sowohl für die USV-Geräte als auch die Clients sollte ein Überspannungsschutz vorhanden sein [SYS2.1.A39]. **Hinweis:** Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV sollte regelmäßig getestet werden. Die USV sollte regelmäßig gewartet werden. **Tipp:** Notebooks enthalten einen Akku, der eine plötzliche Unterbrechung der Stromversorgung ohne großen Aufwand kompensieren kann. Ein Überspannungsschutz ist bei dieser Variante aber weiterhin erforderlich.	☐
E	**Regelmäßige Betriebsdokumentation** Die Durchführung von betrieblichen Aufgaben an Clients sollte nachvollziehbar dokumentiert werden (Wer? Wann? Was?). Aus der Dokumentation heraus sollten insbesondere Konfigurationsänderungen nachvollziehbar sein. Auch Aufgaben (wer ist z. B. befugt, Änderungen durchzuführen) sollten festgelegt und dokumentiert werden. Die Dokumentation sollte gegen unbefugten Zugriff und Verlust geschützt werden [SYS2.1.A40].	☐

Computersysteme in mobilen Befehlsstellen (z.B. Tablets /Laptop / Notebooksystem (Windows 10 Professional)

P/E	Anforderung	Umgesetzt? (Ja/Nein)
P	**Zusätzlich zu den Anforderungen für Computersysteme (Siehe oben) gelten die hier aufgeführten Vorgaben.** **Hinweis!** Aufgrund der leichteren Mobilität eines Laptops / Notebooks werden zusätzliche Anforderungen als verpflichtend deklariert, welche im Bereich „Computersysteme“ nur als Empfehlung genannt wurden. Die zusätzlich verpflichtenden Maßnahmen sind bei Notebooks / Laptops umzusetzen und werden deshalb nochmals erwähnt..	☐
P	**Benutzerauthentisierung** Der Zugriffschutz auf das Betriebssystem (z.B. durch Abfrage von Benutzername und Passwort, Smartcard o.ä.) ist umzusetzen, um den Zugang zu sensiblen Anwendungen und den Zugriff auf vertrauliche Daten in unsicheren Arbeitsumgebungen für Unberechtigte zu erschweren [SYS2.1.A1; SYS2.2.3.A17; SYS3.1.A2].	☐
P	**Bildschirmsperre** Es ist eine Bildschirmsperre mit Zugriffsschutz einzurichten, die nach einer gewissen Zeit automatisiert den Computerzugriff sperrt und zur Reaktivierung eine Benutzerauthentifizierung verlangt. Die Benutzer sind angehalten, beim Verlassen des mobilen Arbeitsplatzes den Computer zu sperren [SYS2.1.A5]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Absicherung des Boot-Vorgangs** Der Startvorgang des Computersystems, dass sogenannte "Booten" muss gegen Manipulationen abgesichert werden. Dafür muss vom Administrator vor Ort festgelegt werden, von welchen Medien gebootet werden darf. Es ist sicherzustellen, dass nur Administratoren die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können [SYS2.1.A8; SYS2.1.A36]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐

P	**Verschlüsselung des Laptops / Notebooks** Wenn vertrauliche Informationen auf dem Computersystem gespeichert werden, z.B. Einsatzberichte als PDF-Datei o.ä., sollten die schutzbedürftigen Dateien, ausgewählte Dateisystembereiche oder besser die gesamte Festplatte verschlüsselt werden [SYS2.1.A28, SYS2.2.3.A21; SYS3.1.A13]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Personal-Firewall** Auf dem Betriebssystem des Befehlsstellenclients sollte die Personal Firewall aktiv sein. Die Filterregeln der Firewall sollten so restriktiv wie möglich sein. Sie sind regelmäßig zu testen. Die Personal Firewall ist so zu konfigurieren, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können [SYS 2.1.A31; SYS3.1.A3]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
E	**Geeignete Aufbewahrung und Diebstahlschutz von Laptops / Notebooks** Es sollten klare Regeln festgelegt werden, wie das Laptop / Notebook bei Nichtnutzung außerhalb der Befehlsstelle aufzubewahren ist. Auch innerhalb der Befehlsstelle sollte außerhalb der Nutzungszeiten das Gerät gegen Diebstahl gesichert und folgerichtig verschlossen aufbewahrt werden [SYS3.1.A14; SYS3.1.A18].	☐

Netzwerktechnik / Router

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Geeignete Aufstellung** Das Endgerät ist so aufzustellen, dass möglichst nur befugte Personen einen Zutritt erhalten.	☐
E	**Unterbrechungsfreie Stromversorgung** Das Endgerät sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Sowohl für die USV-Geräte als auch für die gesamte Netzwerktechnik sollte ein Überspannungsschutz vorhanden sein. **Hinweis:** Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV sollte regelmäßig getestet werden. Die USV sollte regelmäßig gewartet werden.	☐

Drucker / Multi-Funktions-Center / Faxgerät

P/E	Anforderung	**Umgesetzt? (Ja/Nein)**
P	**Anbindung an zentralen Zeitgeber (NTP-Server)** Netzwerkfähige Drucker und Multifunktionsgeräte im Befehlsstellennetz sind an den zentralen Zeitserver der IRLS Lausitz anzubinden. Damit wird die Datenintegrität sichergestellt und Widersprüche vermieden, indem die identische Zeit auf Ausdrucken bereitgestellt wird. **Hinweis:** Genauere Informationen zur Realisierung finden Sie vermutlich in der Bedienungsanleitung des Druckers.	☐
P	**Regelmäßige Aktualisierung** Es ist regelmäßig zu prüfen, ob der Drucker bzw. das Multifunktionscenter auf dem aktuellen Stand ist. Beim Einspielen von Patches und Updates ist darauf zu achten, dass die Aktualisierungen von vertrauenswürdigen Quellen stammen [SYS4.1.A3].	☐
P	**Beschränkung der Administrationszugriffe** Der Zugriff auf die Konfiguration des Endgerätes ist zu beschränken. Dazu ist das Standardpasswort bei Auslieferung zu ändern [SYS4.1.A7].	☐
P	**Verschlüsselte Verbindung** Um Alarmausdrucke von der Leitstelle zu erhalten, ist die Anbindung an den Druckserver der IRLS Lausitz über das Internet-Printing-Protocol-Secure (IPPS) zulässig [SYS4.1.A7]. **Hinweis:** Genauere Informationen zur Umsetzung finden Sie im **Kapitel 7** *Konfiguration und Wartung* des Betriebshandbuchs zum Befehlsstellensystem in der Lausitz.	☐
P	**Sichere Außerbetriebnahme** Bevor Drucker bzw. Multifunktionsgeräte entsorgt, zurückgegeben oder ausgetauscht werden, sind die auf ihnen befindlichen Informationen zu löschen. Dazu ist mindestens die Werkseinstellung zu konfigurieren [SYS4.1.A13].	☐
E	**Geeignete Aufstellung** Das Endgerät ist so aufzustellen, dass möglichst nur befugte Personen einen Zutritt erhalten. Es sollte zumindest nicht in Bereichen aufgestellt werden, in denen sich häufig externe Personen, z.B. Gäste aufhalten. Also zum Beispiel nicht oder in der Nähe von Besprechungs- oder Schulungsräumen [SYS4.1.A2].	☐

E	**Versorgung und Kontrolle der Verbrauchsgüter** Drucker, Kopierer und Multifunktionsgeräte sind auf Verbrauchsgüter wie Papier oder Toner angewiesen, um funktionieren zu können. Die Versorgung mit diesen Verbrauchsgütern sollte in der Befehlsstelle sichergestellt sein. Die Entsorgung der Verbrauchsgüter sollte geregelt werden [SYS4.1.A8].	☐
E	**Protokollierung** Drucker und Multifunktionsgeräte nach Stand der Technik bieten Techniken zur Protokollierung ihrer Nutzung und ermöglichen somit nachträglich eine vereinfachte Störungs- und Fehleranalyse. Die Speicherung von Protokolldaten ist auf maximal 6 Monate zu begrenzen [SYS4.1.A9].	☐
E	**Unterbrechungsfreie Stromversorgung** Das Endgerät sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Sowohl für die USV-Geräte als auch für den Drucker bzw. das Multifunktionsgerät sollte ein Überspannungsschutz vorhanden sein. **Hinweis:** Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV sollte regelmäßig getestet werden. Die USV sollte regelmäßig gewartet werden.	☐
E	**Ordnungsgemäße Entsorgung** Zur Entsorgung von nicht mehr benötigten vertraulichen Ausdrucken, z.B. Einsatzberichte, sollten geeignete Entsorgungseinrichtungen vorhanden und betriebsfähig sein, z.B. Aktenvernichter. Wird das vertrauliche Material zunächst gesammelt und später entsorgt, sollte dieser von unberechtigtem Zugriff geschützt werden [SYS4.1.A12].	☐