

# Spezifische Sicherheitsanforderungen an Endgeräte

Vertraulichkeitsklasse: None (C1)

<b>1</b>	<b>EINLEITUNG</b>	<b>3</b>
1.1	Geltungsbereich	3
1.2	Einschränkungen	3
1.3	Einhaltung des Dokuments durch den Auftragnehmer	3
<b>2</b>	<b>ALLGEMEIN</b>	<b>3</b>
2.1	Benutzerauthentisierung	3
2.2	Rollentrennung und Restriktive Rechtevergabe	4
2.3	Updates und Patches für Firmware, Betriebssystem und Anwendungen	4
2.4	Schutz vor Schadsoftware	4
2.5	Protokollierung	5
2.6	Systemhärtung	5
2.7	Benutzerrichtlinie zur sicheren IT-Nutzung	5
2.8	Geregelte Außerbetriebnahme eines Clients	6
2.9	Verhaltensregeln bei Sicherheitsvorfällen	6
2.10	Private Endgeräte	6
<b>3</b>	<b>NICHT-STATIONÄRE ENDGERÄTE</b>	<b>7</b>
3.1	Verschlüsselung der Endgeräte	7
3.2	Personal Firewall	7
<b>4</b>	<b>MOBILE ENDGERÄTE</b>	<b>7</b>
4.1	Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten	7
4.2	Verwendung eines Zugriffsschutzes	7
4.3	Installation und Updates von Betriebssystem und Apps	7
4.4	Deaktivierung nicht benutzter Kommunikationsschnittstellen	8

# 1 Einleitung

Informationen sind wichtige Unternehmenswerte für Stromnetz Berlin GmbH und im Rahmen dieser Vereinbarung wird der Auftragnehmer/Dienstleister (im Weiteren bezeichnet als „Auftragnehmer“) Zugriff auf Informationen vom Auftraggeber und seiner Partner (im Weiteren bezeichnet als „Auftraggeber-Informationen“) erhalten sowie verarbeiten. Zur Minimierung der Informationssicherheitsrisiken und Sicherstellung, dass Auftraggeber-Informationen angemessen geschützt werden, pflegt der Auftraggeber ein Regelwerk aus Richtlinien und Verfahrensanweisungen, welches auf alle Informationen und Informationsdienste anzuwenden ist.

Dieses Dokument beinhaltet die spezifischen Auftraggeber Sicherheitsanforderungen an Endgeräte, die durch den Auftragnehmer für die Verarbeitung von Auftraggeber Informationen zum Einsatz kommen.

## 1.1 Geltungsbereich

Auftraggeber Anforderungen an die Informationssicherheit (Verpflichtungen des Auftragnehmers) beziehungsweise dem Datenschutz gelten für alle Auftraggeber-Informationen (z. B. Projektdaten, Kunden- oder produktbezogene Daten) beziehungsweise personenbezogene Daten die Vertragsgegenstand sind.

Der Auftragnehmer ist über die gesamte in seiner Sphäre liegende Zulieferkette verantwortlich für die Einhaltung der Informationssicherheits- und Datenschutzanforderungen (insbesondere für die vom Auftragnehmer etwaig eingesetzten Unterauftragnehmer).

Im Geltungsbereich dieses Dokument bezeichnet der Begriff Endgerät oder auch Client ein für die Nutzung durch Endanwender vorgesehenes IT-System, welches das Personal des Auftragnehmers für die Verarbeitung von Auftraggeber-Informationen nutzt.

## 1.2 Einschränkungen

Werden in diesem Dokument Anforderungen beschrieben, die im Rahmen des Vertragsgegenstands nicht anwendbar sind, so muss der Dienstleister diese Anforderungen nicht erfüllen.

## 1.3 Einhaltung des Dokuments durch den Auftragnehmer

Potentielle Abweichungen zu den in diesem Dokument aufgeführten Anforderungen sind durch den Dienstleister vor Vertragsunterzeichnung zuzüglich einer Liste nicht-anwendbarer Anforderungen (siehe 1.2 ) schriftlich zu dokumentieren und bereitzustellen.

Nach Aufforderung durch den Auftraggeber hat der Auftragnehmer durch die Bereitstellung angemessener Nachweise die Einhaltung der Anforderungen und Vorgaben nachzuweisen. Die Nachweise haben sich auch auf die durch den Auftragnehmer beauftragten Unterauftragnehmer zu erstrecken.

Jedwede Verletzung der Anforderungen in diesem Dokument durch den Auftragnehmer oder einem seiner Unterauftragnehmer kann in der Begrenzung des Zugangs zu Auftraggeber-Informationen oder Informationsdiensten oder der sofortigen Beendigung des Vertrages führen.

# 2 Allgemein

Die nachfolgenden Sicherheitsanforderungen gelten sowohl für stationäre als auch nicht-stationäre Endgeräte jeglichen Typs, wie zum Beispiel Desktop-Rechner, Laptop, Notebook, Tablets oder Smartphone.

## 2.1 Benutzerauthentisierung

- (1) Um das Endgerät zu nutzen, müssen sich die Benutzer gegenüber dem Endgerät oder einem zentralen Authentisierungssystem authentisieren.

- (2) Werden für die Benutzerauthentisierung Passwörter verwendet, müssen sichere Passwörter benutzt werden. Der Auftragnehmer hat hierfür eine Passwort-Richtlinie zu etablieren und durchzusetzen.
- (3) Eine Bildschirmsperre muss verwendet werden, damit keine Unbefugten auf die aktivierten Endgeräte zugreifen können. Sie sollte sich sowohl manuell vom Benutzer aktivieren lassen als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch gestartet werden. Es muss sichergestellt sein, dass die Bildschirmsperre erst nach einer erfolgreichen Benutzerauthentifikation deaktiviert werden kann.
- (4) Es müssen alle Benutzer verpflichtet werden, sich nach Aufgabenerfüllung vom Endgeräte bzw. von der IT-Anwendung abzumelden, vor allem bei Nutzung eines Systems durch mehrere Benutzer. Ist für einen Benutzer absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, muss die Bildschirmsperre aktiviert werden.

## **2.2 Rollentrennung und Restriktive Rechtevergabe**

- (1) Das Endgerät muss so eingerichtet werden, dass normale Tätigkeiten nicht mit Administrationsrechten erfolgen. Nur Administratoren dürfen Administrationsrechte erhalten. Es dürfen nur Administratoren die Systemkonfiguration ändern, Anwendungen installieren bzw. entfernen oder Systemdateien modifizieren bzw. löschen können. Benutzer dürfen ausschließlich lesenden Zugriff auf Systemdateien haben. Auch System-Verzeichnisse sollten nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.
- (2) Der verfügbare Funktionsumfang des Endgeräts sollte für einzelne Benutzer oder Benutzergruppen eingeschränkt werden, sodass sie genau die Rechte besitzen und auf die Funktionen zugreifen können, die sie für ihre Aufgabenwahrnehmung benötigen. Zugriffsberechtigungen sollten hierfür möglichst restriktiv vergeben werden.
- (3) Der Kreis der zugriffsberechtigten Administratoren ist möglichst klein zu halten. Der Zugriff auf Internet oder auf E-Mails ist für administrative Kennungen zu unterbinden.

## **2.3 Updates und Patches für Firmware, Betriebssystem und Anwendungen**

- (1) Automatische Update-Mechanismen (Autoupdate) müssen aktiviert werden, sofern nicht andere Mechanismen wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden. Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, sollte mindestens täglich automatisch nach Updates gesucht und diese installiert werden.
- (2) Administratoren müssen sich regelmäßig über bekannt gewordene Schwachstellen informieren. Die identifizierten Schwachstellen müssen so schnell wie möglich behoben werden, Updates und Patches müssen so schnell wie möglich eingespielt werden. Generell sollte darauf geachtet werden, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden. Solange keine entsprechenden Patches zur Verfügung stehen, sollten abhängig von der Schwere der Schwachstellen andere geeignete Maßnahmen zum Schutz der Endgeräte getroffen werden.

## **2.4 Schutz vor Schadsoftware**

- (1) In Abhängigkeit vom installierten Betriebssystem und andere vorhandenen Schutzmechanismen des Clients muss eine spezialisierte Komponente zum Schutz vor Schadsoftware eingesetzt werden. Für Windows-basierte Systeme ist der Einsatz eines Viren-Schutzprogrammes verpflichtend.
- (2) Es muss sichergestellt werden, dass sowohl das Scan-Programm als auch die Signaturen stets auf dem aktuellsten Stand sind. Viren-Schutzprogramme auf den Endgeräten müssen so konfiguriert sein, dass die Benutzer weder sicherheitsrelevante Änderungen an den Einstellungen vornehmen können noch diese deaktivieren können.

## 2.5 Protokollierung

- (1) Alle sicherheitsrelevanten Systemereignisse, wie zum Beispiel erfolgreiche oder erfolglose Anmeldungen beziehungsweise Anmeldeversuche, müssen protokolliert werden. Die Protokolle dürfen durch die Benutzer nicht manipuliert werden können.

## 2.6 Systemhärtung

- (1) Alle Endgeräte müssen so konfiguriert sein, dass sie den erforderlichen Schutzbedarf angemessen erfüllen. Dafür muss eine passende Grundkonfiguration zusammengestellt und dokumentiert werden.
- (2) Es sollte festgelegt werden, welche Komponenten des Betriebssystems, Fachanwendungen und weitere Tools installiert werden sollen. Die Installation und Konfiguration der Endgeräte darf nur von autorisierten Personen (Administratoren oder vertraglich gebundene Dienstleister) nach einem definierten Prozess durchgeführt werden.
- (3) Nach beziehungsweise während der Installation muss überprüft werden, welche Komponenten der Firmware, des Betriebssystems, welche Anwendungen und weiteren Tools auf den Clients installiert und aktiviert sind. Nicht benötigte Module, Programme, Dienste, Benutzerkennungen und Schnittstellen sind zu deaktivieren oder sollten ganz deinstalliert werden. Außerdem sollten nicht benötigte Laufzeitumgebungen, Interpretersprachen und Compiler deinstalliert werden. Entsprechende nicht benötigte, jedoch fest mit dem Endgerät verbundene Komponenten sollten deaktiviert werden. Auch in der Firmware vorhandene nicht benötigte Komponenten (z.B. Diebstahlschutz, Fernwartung) sollten abgeschaltet werden. Es sollte verhindert werden, dass diese Komponenten wieder reaktiviert werden können.

Die Grundeinstellungen von Clients sollten überprüft und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden.

- (4) Der Startvorgang des Endgerätes ("Booten") muss gegen Manipulation abgesichert werden. Es muss festgelegt werden, von welchen Medien gebootet werden darf. Es sollte entschieden werden, ob und wie der Bootvorgang kryptografisch geschützt werden soll. Es muss sichergestellt werden, dass nur Administratoren die Endgeräte von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können. Nur Administratoren dürfen von eingebauten optischen oder externen Speichermedien booten können. Die Konfigurationseinstellungen des Boot-Vorgangs Firmware dürfen nur durch Benutzer mit administrativen Rechten verändert werden können.
- (5) Abhängig davon, ob Endgeräte lokal, über das Netz oder über zentrale netzbasierte Tools administriert werden, sind geeignete Sicherheitsvorkehrungen zu treffen. Die Administration über das Netz muss über sichere Protokolle erfolgen.
- (6) Es sollte technisch oder organisatorisch verhindert werden, dass auf Endgeräten von Laufwerken oder über sonstige Netzwerk- oder Geräteschnittstellen unkontrolliert Software installiert oder unberechtigt Daten kopiert werden können. Es sollte generell verhindert werden, dass von den Endgeräten auf Daten aus nicht vertrauenswürdigen Quellen zugegriffen wird.
- (7) Nicht benutzte Kommunikationsschnittstellen sollten deaktiviert werden. Notwendige Schnittstellen sollten nur in geeigneten Umgebungen aktiviert sein.

## 2.7 Benutzerrichtlinie zur sicheren IT-Nutzung

- (1) Es sollte eine Richtlinie erstellt werden, in der für alle Mitarbeiter transparent beschrieben wird, welche Rahmenbedingungen bei der IT-Nutzung eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie sollte folgende Punkte abdecken:
  - Sicherheitsziele

- Wichtige Begriffe
- Aufgaben und Rollen mit Bezug zur Informationssicherheit
- Ansprechpartner zu Fragen der Informationssicherheit
- Von den Mitarbeitern umzusetzende und einzuhaltende Sicherheitsmaßnahmen

## **2.8 Regelte Außerbetriebnahme eines Clients**

- (1) Bei der Außerbetriebnahme eines Endgeräts muss sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen und dass keine sensiblen Daten zurückbleiben. Es sollte eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines IT-Systems abgearbeitet werden kann. Diese Checkliste sollte mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.
- (2) Der Auftragnehmer hat auf Verlangen durch den Auftraggeber adäquate Nachweise über die sichere Außerbetriebnahme inklusive des sicheren Lösches der auf den Endgeräten befindlichen Auftraggeber Informationen bereitzustellen.

## **2.9 Verhaltensregeln bei Sicherheitsvorfällen**

- (1) Generell müssen alle Sicherheitsvorfälle gemeldet und behandelt werden. Gehen Geräte verloren oder werden unberechtigt Änderungen an Gerät und Software festgestellt, muss der Auftragnehmer sofort geeignete Gegenmaßnahmen einleiten.
- (2) Die möglichen Konsequenzen sicherheitskritischer Ereignisse müssen untersucht werden. Alle erforderlichen Maßnahmen müssen ergriffen werden, um auszuschließen, dass auf vertrauliche und geschäftskritische Informationen des Auftraggebers zugegriffen werden kann.
- (3) In jedem Fall sind Sicherheitsvorfälle, die Auftraggeber-Informationen betreffen, unverzüglich dem Auftraggeber zu melden und die Ergebnisse der Untersuchungen der Vorfälle bereitzustellen.

## **2.10 Private Endgeräte**

- (1) Die Nutzung privater Endgeräte - auch Bring Your Own Device Konzepte genannt - für die Verarbeitung von Auftraggeber-Informationen ist im Regelfall nicht gestattet sondern nur in Ausnahmefällen und nach Freigabe durch den Auftraggeber.
- (2) Ausnahmen erfordern Installation und Betrieb eines zentral konfigurierten und gesteuerten Mobile Device Management (MDM) oder Enterprise Mobile Management (EMM) Systems und einer Verwaltungssoftware auf den betroffenen Endgeräten. Funktionalität und Konfiguration des MDM Systems sind dem Auftraggeber im Detail darzulegen.
- (3) Die Deinstallation der Verwaltungssoftware des MDM Systems oder das Rooten des Geräts muss technisch durch das MDM unterbunden werden beziehungsweise zu einer automatischen Löschung der geschäftlichen Daten auf dem privaten Endgerät führen.
- (4) Es muss eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von privaten Endgeräten erstellt und von den betroffenen Mitarbeitern unterzeichnet werden. Diese muss unter anderem festlegen, wie private Geräte genutzt und gepflegt werden sollen. Die Themen Aufbewahrung, Verlustmeldung, Reparatur, Ausschied aus dem Unternehmen und die damit verbundenen Pflichten des Mitarbeiters und Rechte des Auftragnehmers (in seiner Arbeitgeberrolle) müssen ebenfalls betrachtet werden.

## 3 Nicht-Stationäre Endgeräte

Die nachfolgenden Sicherheitsanforderungen gelten neben den allgemeinen Anforderungen für alle Endgeräte, die - zu mindestens zeitweise - mit öffentlichen Netzwerken oder Netzwerken Dritter verbunden werden oder sich außerhalb der geschützten Räumlichkeiten des Auftragnehmers oder des Auftraggebers befinden beziehungsweise genutzt werden. Dies trifft in der Regel auf den Einsatz nicht-stationärer Endgeräten, wie Notebooks oder Laptops, sowie mobiler Endgeräte (siehe 4 ), wie Smartphones oder Tablets, zu.

### 3.1 Verschlüsselung der Endgeräte

- (1) Nicht-stationäre Endgeräte müssen verschlüsselt werden. Für die Verschlüsselung muss ein sicherer Verschlüsselungsalgorithmus eingesetzt werden. Die Schlüssel müssen zufällig erzeugt und Daten und Schlüssel getrennt aufbewahrt werden. Es muss sichergestellt sein, dass die Wiederherstellungsinformationen nur berechtigten Personen zugänglich sind. Das verwendete Schlüsselmaterial darf nicht im Klartext auf den Endgeräten gespeichert sein.
- (2) Eventuell vorhandene Speichererweiterungen, wie zum Beispiel SD-Karten, müssen ebenfalls verschlüsselt werden.

### 3.2 Personal Firewall

- (1) Auf Notebooks bzw. Laptops muss eine Personal Firewall aktiv sein. Die Filterregeln der Firewall müssen so restriktiv wie möglich sein.

## 4 Mobile Endgeräte

Die nachfolgenden Sicherheitsanforderungen gelten für den Einsatz so genannter mobiler Endgeräte, wie Smartphones oder Tablets, die - unter anderem - dadurch gekennzeichnet sind, dass Sie mit einem mobilen Betriebssystem wie zum Beispiel Android, Apple iOS ausgestattet sind.

### 4.1 Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten

- (1) Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden. Diese sollte festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. Darin sollten die Themen Aufbewahrung und Verlustmeldung behandelt werden. Außerdem sollte klar verboten werden, Verwaltungssoftware zu deinstallieren oder das Gerät zu rooten.

### 4.2 Verwendung eines Zugriffsschutzes

- (1) Es müssen alle mobilen Endgeräte mit einem Gerätesperrcode geschützt werden. Die Nutzung der Bildschirmsperre muss vorgeschrieben werden.
- (2) Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm muss deaktiviert sein. Alle mobilen Geräte müssen nach wenigen Minuten selbsttätig den Bildschirm sperren. Die Nutzung trivialer Gerätecodes ist zu unterbinden.

### 4.3 Installation und Updates von Betriebssystem und Apps

- (1) Verfügbare Updates des Betriebssystems und der eingesetzten Apps müssen zeitnah installiert werden.
- (2) Bereits bei der Auswahl von zu beschaffenden mobilen Geräten muss der Auftragnehmer darauf achten, dass der Hersteller über den geplanten Nutzungszeitraum Updates für die Geräte bereitstellt.
- (3) Ältere Geräte, für die keine aktuellen Versionen mehr bereitgestellt werden, müssen ausgesondert und durch vom Hersteller unterstützte Geräte ersetzt werden.

- (4) Die Installation von Apps aus alternativen beziehungsweise nicht offiziellen Märkten muss unterbunden werden.
- (5) Die Installation von Apps aus dem Dateisystem muss unterbunden werden.
- (6) Apps aus offiziellen aber öffentlichen App-Stores sollten geprüft und freigegeben werden. Dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden.

#### **4.4 Deaktivierung nicht benutzter Kommunikationsschnittstellen**

- (1) Nicht benutzte Kommunikationsschnittstellen sollten deaktiviert werden. Notwendige Schnittstellen sollten nur in geeigneten Umgebungen aktiviert sein.