

TLP: Green

# Handlungsleitfaden für die Nutzung von WLAN an der HSF Meissen



## Dokumenteninformation

|                            |   |
|----------------------------|---|
| <b>Titel des Dokuments</b> | Handlungsleitfaden für die Nutzung von WLAN an der HSF Meißen             |
| <b>Version</b>             | 1.0   |
| <b>Klassifikation</b>      | <b>TLP-Green</b>  |
| <b>Verteilerkreis</b>      | alle Mitarbeiter, Dozenten und Gäste                                      |
| <b>Gültigkeitszeit</b>     | Unbegrenzt  |
| <b>Dateiname</b>           | Handlungsleitfaden für die WLAN Nutzung an der HSF Meißen_2021-02-17.docx |
| <b>Ablageort</b>           | P:\WLAN\WLAN-Richtlinie HSF-Meißen  |

|                                   |                    |
|-----------------------------------|--------------------|
| <b>Dokumentenverantwortlicher</b> | HSF Referent ZIT   |
| <b>Freigabe durch</b>             | Referatsleiter ZIT |
| <b>letzte Überarbeitung</b>       | 02/2021            |
| <b>Überarbeitungsintervall</b>    | 2 Jahre            |

| <b>Versionshistorie</b> |                |  |                   |
|-------------------------|----------------|--|-------------------|
| <b>Datum:</b>           | <b>Version</b> | <b>Beschreibung</b>                            | <b>Bearbeiter</b> |
| 04.09.2020              | 0.1            | Initiale Erstellung aus Handlungsleitfaden SID | Prax              |
| 01.10.2020              |                | WLAN-AD Gruppenerstellung dokumentiert         |                   |
| 09.10.2020              |                | Formulierungen, technische Aspekte             | Muskulus          |
| 20.10.2020              | 0.2            | Überarbeitung, Redundanzen vermieden           | Prax              |
| 27.10.2020              | 0.3            | Prüfung, mit Änderungen                        | Rudolf            |
| 10.11.2020              | 0.5            | Aktualisierung Anl. 3                          | Prax              |
|                         | 0.6            | Formatierung Layout                            | Muskulus          |
| 23.12.2020              | 0.9            | Überarbeitung zur Zeichnung                    | Prax              |
| 17.02.2021              | 1.0            | Redakt. Überarbeitung und Freigabe             | Prax              |

## Inhalt

|           |  |           |
|-----------|--|-----------|
| <b>1.</b> | <b>Zielsetzung des Dokuments .....</b>   | <b>4</b>  |
| <b>2.</b> | <b>Rahmenbedingungen der WLAN-Nutzung .....</b>  | <b>5</b>  |
| 2.1.      | Überblick der WLAN-Architektur, Nutzergruppen und Kommunikationswege.....                                | 5         |
| 2.2.      | Landesbedienstete am fremden Behördenstandort.....   | 6         |
| 2.3.      | Landesbedienstete am eigenen Behördenstandort.....   | 6         |
| 2.4.      | Gast-Nutzer bzw. Mitarbeiter mit nicht verwalteten Endgeräten .....                                      | 6         |
| 2.5.      | eduroam-Nutzer am Standort der HSF .....   | 7         |
| <b>3.</b> | <b>WLAN-Anbindung dienstlich verwalteter Endgeräte .....</b>   | <b>8</b>  |
| 3.1.      | Einsatzzweck.....  | 8         |
| 3.2.      | Organisatorischer Ablauf für die Einbindung in das WLAN .....  | 8         |
| <b>4.</b> | <b>WLAN für nicht dienstlich verwaltete und private<br/>Endgeräte über das Self-Service-Portal .....</b> | <b>9</b>  |
| 4.1.      | Einsatzzweck.....  | 9         |
| 4.2.      | Organisatorischer Ablauf der Ticketerstellung.....   | 9         |
| <b>5.</b> | <b>WLAN für Gäste der HSF über das WLAN-Gast-Portal ...</b>  | <b>10</b> |
| 5.1.      | Einsatzzweck.....  | 10        |
| 5.2.      | Organisatorischer Ablauf der Ticketerstellung.....   | 10        |
| <b>6.</b> | <b>Nutzungsbedingungen und Datenschutz .....</b>   | <b>11</b> |
| <b>7.</b> | <b>Fehlerbehebung .....</b>  | <b>11</b> |
| <b>8.</b> | <b>Anhang.....</b>   | <b>12</b> |
|           | Abkürzungsverzeichnis.....   | 12        |
|           | Allgemeine Nutzungsbedingungen für die kostenlose Internetnutzung .....                                  | 13        |
|           | Datenschutzbestimmungen .....  | 15        |
|           | Erstellen und Verwalten von WLAN-Tickets Handlungsanleitung .....  | 18        |

# 1. Zielsetzung des Dokuments

Dieser Handlungsleitfaden beschreibt die Einführung und Nutzung von WLAN an der Hochschule Meißen (FH) und Fortbildungszentrum (HSF). Die einzelnen Rahmenbedingungen, Regelungen und Anleitungen orientieren sich an dem „Handlungsleitfaden für die WLAN-Nutzung im SVN 2.0“ des Staatsbetriebs Sächsische Informatik Dienste (SID).

In diesem Dokument sind zum einen die für die HSF relevanten Rahmenbedingungen für die Einführung und Nutzung von WLAN aufgeführt. Neben der Schilderung der grundsätzlich bereitgestellten Funktionalitäten, Verantwortlichkeiten und Nutzungshinweisen sind in diesem Handlungsleitfaden ebenso der Beantragungsweg für Zugänge aufgeführt. Darüber hinaus enthält dieses Dokument die Handlungsanleitung für die Erstellung und Verwaltung der WLAN-Tickets. Den Nutzern soll damit ein Überblick über die Art und Weise der Bereitstellung von WLAN am Campus der HSF Meißen zur Verfügung gestellt werden. Die Aufgaben bzw. Konfigurationsschritte der HSF Meißen für die Nutzung von WLAN als Dienstleistung des SID sowie die durch das Zentrum für Informationstechnologie der HSF (ZIT) nötigen Konfigurationsaspekte werden in einem separaten Dokument zu Dokumentation der WLAN-Umgebung festgehalten.

| WLAN an der HSF Meißen   |                                     |
|--|-------------------------------------|
| Dokument 1   | Dokument 2                          |
| Handlungsleitfaden   | Konfigurationsdokumentation         |
| Inhalt:<br>Beschreibung der WLAN-Umgebung für die Nutzer, inkl. Beantragungswege für Zugänge | Inhalt:<br>Technische Dokumentation |

## 2. Rahmenbedingungen der WLAN-Nutzung

### 2.1. Überblick der WLAN-Architektur, Nutzergruppen und Kommunikationswege

Dieses Kapitel umfasst grundlegende Rahmenbedingungen für die WLAN-Nutzung an der HSF Meißen.

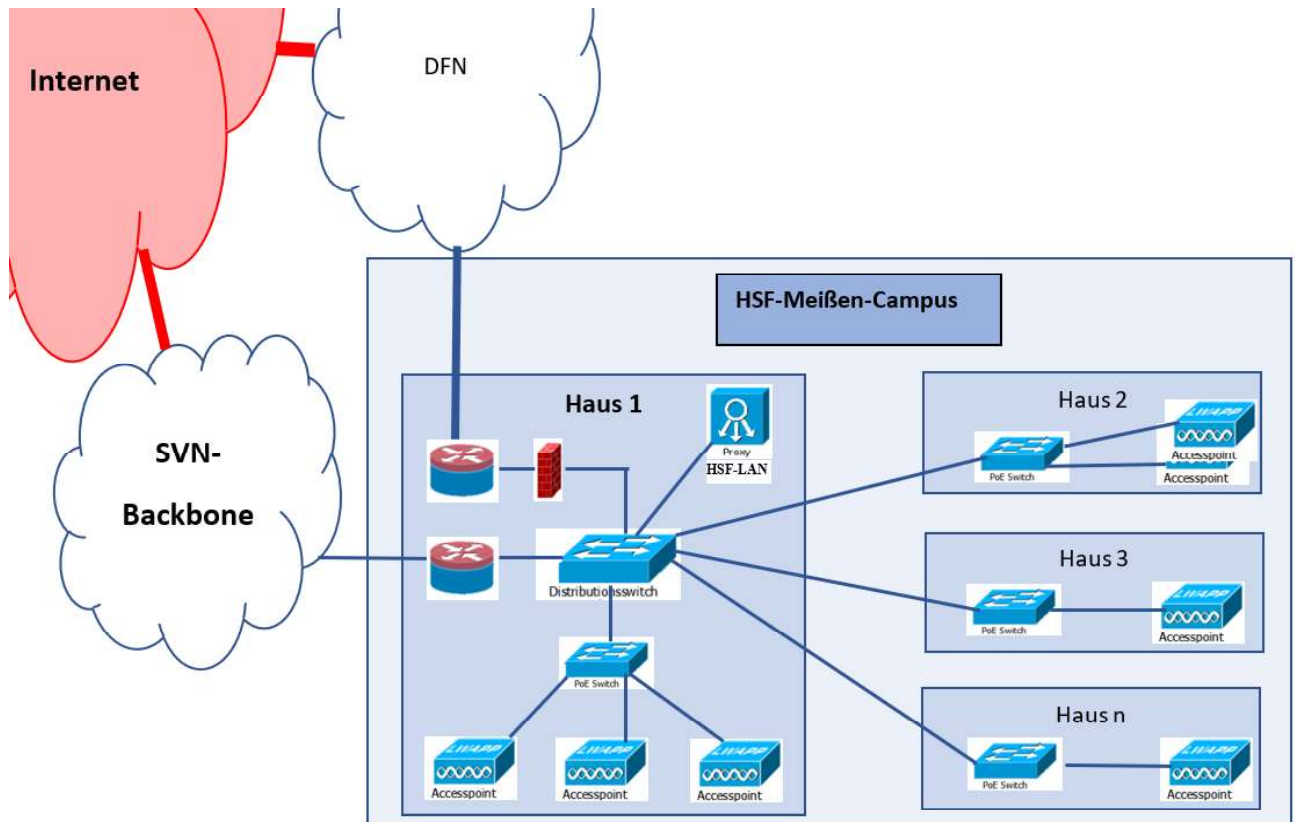


Abbildung 1: Überblick über die WLAN-Architektur der HSF Meißen

Für die Realisierung der drahtlosen Kommunikation über WLAN sind drei unterschiedliche, parallel bereitgestellte Zugänge zu differenzieren:

1. „**SVN-WLAN**“ für das mobile Arbeiten von Landesbediensteten mit Zugriff auf SVN-interne Ressourcen ihrer jeweiligen Behörde
2. „**SVN-GastNetz**“ für den Internetzugang ohne Zugriff auf SVN-Ressourcen und interne Behördendienste. Hierbei ist zwischen zwei Nutzerklassen zu unterscheiden:
  - a. WLAN-Zugang für Mitarbeiter
  - b. WLAN-Zugang für Gäste
3. „**eduroam-WLAN**“ für Studenten und Dozenten der HSF, als auch für externe Nutzer von nationalen und internationalen Bildungs- und Forschungseinrichtungen, die am Deutschen Forschungsnetz (DFN) bzw. EDUROAM-Netzwerk teilnehmen. Das Netz bietet Zugriff auf das Internet über die DFN-Infrastruktur, als auch auf Dienste der DFN-Infrastruktur. **[geplant]**

Alle drei Realisierungsformen werden durch die in Abbildung 1 dargestellte Infrastruktur zur Verfügung gestellt.

Eine Kommunikation zwischen Endgeräten in den unterschiedlichen WLAN-Netzen findet nicht statt. Die Netze sind miteinander nicht verbunden. Zusammengefasst ergeben sich abhängig vom jeweiligen Nutzer vier verschiedene Kommunikationsszenarien am Campus:

- Landesbedienstete des Freistaats an fremden Behördenstandort mit Zugriff auf ihr eigenes Behörden-Netz mit einem dienstlich verwalteten Endgerät,
- Landesbedienstete des Freistaats am eigenen Behördenstandort mit Zugriff auf ihr Behörden-Netz mit einem dienstlich verwalteten Endgerät,
- Gast-Nutzer und Mitarbeiter mit ausschließlichem Zugang zum Internet über das SVN und
- Angehörige von Bildungs- und Forschungseinrichtungen, die am weltweiten eduroam-Netzwerk teilnehmen (u. a. Studenten und Dozenten der HSF) mit Zugriff auf das Internet über das DFN [geplant]

## 2.2. Landesbedienstete am fremden Behördenstandort

Zur Realisierung des kabellosen, mobilen Arbeitens auch an behördenfremden Standorten wurde ein zentraler virtueller SVN-2.0-Standort im SVN-Backbone geschaffen, der im Weiteren als SINI-WLAN-Campus bezeichnet wird (vgl. Dokumentation SVN-WLAN-Dienst). Am SINI-WLAN-Campus liegt für alle Behördengruppen des SVN 2.0 das jeweilige Behördengruppennetz zentral an. Somit kann der WLAN-Verkehr dort zentral ausgeleitet und in das jeweilige Ressort- bzw. Behördengruppennetz übergeben werden. Hierzu erhalten die einzelnen Netze der Behördengruppen jeweils einen spezifischen IP-Adressbereich, der für die Adressierung der Endgeräte genutzt wird. Landesbedienstete mit Zugang zum **SVN-WLAN** (nur für dienstliche, verwaltete Endgeräte!) können damit auf das jeweilige Behördennetz auch aus anderen Behördenstandorten über das SVN-WLAN zugreifen. Für Nutzer der HSF bedeutet dies, dass sie in anderen Behörden des Freistaates Sachsen das dortige **SVN-WLAN** nutzen können, um in das Verwaltungsnetz der HSF Meißen zuzugreifen. WLAN-Nutzer anderer Behörden können wiederum (ohne weiteres Zutun) das SVN-WLAN am Campus nutzen, um auf ihre Behördennetze zuzugreifen.

## 2.3. Landesbedienstete am eigenen Behördenstandort

Um den Datenverkehr am zentralen SINI-WLAN-Campus zu minimieren, wird der Zugriff auf lokale Daten bereits vor Ort ausgeleitet. Somit erfolgt keine Datenkommunikation über den zentralen SINI-WLAN-Campus und damit keine Nutzung der Bandbreite des SVN-Anschlusses. HSF-Bedienstete werden mit ihrem dienstlich verwalteten Endgerät am Standort HSF genauso lokal in ein definiertes Vor-Ort-VLAN eingeordnet wie andere Behördenmitarbeiter an ihren jeweiligen Standorten. Dadurch erfolgt der Zugriff eines HSF-Mitarbeiters auf die HSF-Daten des per WLAN-angebundenen Nutzers bzw. Endgeräts (nur für dienstliche, verwaltete Endgeräte) ausschließlich am Standort HSF und nicht über die zentralen Komponenten des SINI/SVN.

## 2.4. Gast-Nutzer bzw. Mitarbeiter mit nicht verwalteten Endgeräten

Gast-Nutzer und Mitarbeiter mit nicht verwalteten dienstlichen oder privaten Endgeräten erhalten über das **SVN-GastNetz** durch einen abgesicherten Tunnel ausschließlich Zugriff auf das Internet. Der Zugang zum SVN-Gastnetz wird durch einen separaten WLAN-Controller innerhalb des SVN (Anchor Controller) gesteuert. Dabei sind zwei Zugangsarten zu differenzieren: Mitarbeiter und Studenten greifen mittels Self-Service-Ticket auf das **SVN-GastNetz** zu. Gäste der HSF Meißen greifen mittels Gast-Portal-Ticket auf das **SVN-GastNetz** zu.

Die Kommunikation der Gast-Nutzer und der Bediensteten mit nicht verwalteten dienstlichen bzw. privaten Endgeräten erfolgt ausschließlich ins Internet. Für diese Nutzer ist kein Zugriff auf interne SVN- oder HSF-Ressourcen möglich. Wenn der Nutzer versucht, eine Internetseite aufzurufen, wird diese Anfrage auf eine Anmeldeseite umgelenkt. Hier muss sich der Nutzer mittels Benutzername und Passwort aus dem Ticket authentifizieren. Nach erfolgreicher Anmeldung wird die Kommunikation in das Internet für den Zeitraum der Berechtigung für das jeweilige Endgerät freigeschaltet. Die Adressierung der Endgeräte der Gast-Nutzer erfolgt über eigene, offizielle SVN-Adressen, die jedoch keinem SVN-Dienst zugeordnet sind.

## 2.5. eduroam-Nutzer am Standort der HSF

Eduroam ist ein weltweites WLAN-Roaming-Konsortium, das Mitgliedern von Forschung und Lehre an allen eduroam-Hotspots kostenlosen Zugang zum Internet gibt. Der WLAN-Zugriff ist für Studenten und Bedienstete der HSF, als auch für sämtliche Nutzer der teilnehmenden Organisationen vorgesehen. Die grundsätzliche Verfahrensweise lässt sich wie folgt beschreiben:

Die HSF stellt über einen RADIUS-Server einen Dienst zur Authentifizierung von Benutzerkonten der HSF bereit. Der RADIUS-Server muss weltweit über das Internet erreichbar sein, damit andere Einrichtungen, die am EDUROAM teilnehmen, Authentifizierungsanfragen an ihn senden können. Dafür muss der RADIUS-Server über eine öffentliche IP-Adresse (idealerweise an einem DFN-Anschluss) betrieben werden. Der RADIUS-Server der HSF befragt eine Datenquelle für Benutzerkonten. Dies können das ActiveDirectory AUSBILDUNG und/oder weitere Datenbanken wie ANTRAGO sein.

Die Zugangsdaten der Nutzer zum WLAN eduroam sind dieselben wie für die IT-Infrastruktur an der HSF. Zur Verwendung des WLAN eduroam konfigurieren die Nutzer jedes ihrer Endgeräte einmalig mit dem „eduroam Configuration Assistent Tool“ von <https://cat.eduroam.org>. Danach verbinden sie sich mit der WLAN-SSID. Bei allen folgenden Nutzungen erfolgt der Login automatisiert. Die Datenübertragung im WLAN ist verschlüsselt.

Damit Nutzer das „eduroam Configuration Assistent Tool“ verwenden können, muss die HSF als Identitätsprovider (IdP) beim EDUROAM-Netzwerk registriert sein. Dazu benötigt die HSF eine Einladung vom „Nationalen Roaming Betreiber“, dem DFN e.V. Dann kann die HSF als „Lokaler eduroam CAT Administrator“ ihre Konfigurationsdetails hinterlegen. Daraufhin werden maßgeschneiderte Installationsprogramme für eine Vielzahl von Plattformen (Betriebssysteme) erzeugt. Ein Installationsprogramm für eine Organisation funktioniert nicht für Nutzer einer anderen Organisation.

Bis zur Bereitstellung des eduroam-WLAN werden die Endgeräte der Studenten und Dozenten über das Self-Service-Portal wie die dienstlichen bzw. privaten Endgeräte von Landesbediensteten in das WLAN „SVN-GastNetz“ eingeordnet. Sie verfahren daher wie in Kap. 4 beschrieben.

## 3. WLAN-Anbindung dienstlich verwalteter Endgeräte

### 3.1. Einsatzzweck

Für die Nutzung des WLAN durch dienstliche Endgeräte, die durch die Administration verwaltet werden, müssen entsprechende Voraussetzungen und Einstellungen (Systemproxy, Zertifikate, Gruppenrichtlinien, WLAN-Profile, etc.) für das Endgerät geschaffen werden. Ziel ist die wahlweise Nutzung des Behörden-LAN (drahtgebunden) oder SVN-WLAN am Campus der HSF, als auch des SVN-WLAN an anderen Behördenstandorten zur Verbindung mit den zentralen Behördendiensten. Die dafür nötigen Einstellungen werden zentral durch das ZIT konfiguriert. Ein weiteres Zutun des Nutzers ist nicht erforderlich.

### 3.2. Organisatorischer Ablauf für die Einbindung in das WLAN

Die beabsichtigte Nutzung von bestehenden Endgeräten mit WLAN an der HSF Meißen bzw. an anderen Behördenstandorten mit SVN-WLAN zeigt der Nutzer durch E-Mail an das Postfach [zit@hsf.sachsen.de](mailto:zit@hsf.sachsen.de) an.

Für neu ausgegebene Laptops wird die Nutzung von WLAN bereits initial durch das ZIT bereitgestellt.



# 4. WLAN für nicht dienstlich verwaltete und private Endgeräte über das Self-Service-Portal

## 4.1. Einsatzzweck

Der WLAN-Self-Service dient ausschließlich der Nutzung durch Landesbedienstete. Es ist sicherzustellen, dass der Nutzer auch Landesbediensteter ist. Die mit einem Self-Service-Ticket im WLAN verbundenen Endgeräte können sich frei im Internet bewegen, eine Mitnutzung der landeseigenen Dienste erfolgt nicht. Der WLAN-Self-Service darf nicht Gästen des Freistaat Sachsen zur Verfügung gestellt werden (diese haben nur das Recht der Nutzung des WLAN-Gastzuganges).

Es liegt in der Verantwortung der HSF, dienstlichen, nicht zentral verwalteten Endgeräten einen zeitlich befristeten freien Zugang zum Internet über das Self-Service-Portal zur Verfügung zu stellen. An der HSF trifft dies vor allem auf Laptops, die nicht im Verwaltungsnetz registriert sind, und dienstliche mobile Endgeräte zu. Die sogenannten Self-Service-Tickets (auch als Voucher bezeichnet) werden für maximal 180 Tage ausgestellt, können jedoch verlängert bzw. gesperrt werden.

Die Ausstellung der Self-Service-Tickets erfolgt

| Zugang für                           | Erstellung durch   |
|--------------------------------------|--|
| Mitarbeiter und Dozenten der HSF     | Administratoren des ZIT oder Bedienstete in den Studienorganisationen der Fachbereiche |
| Studenten und nebenamtliche Dozenten | Bedienstete in der Studienorganisation oder den Studentensekretariaten                 |

Für die großen Personengruppen soll erstmalig eine Erstellung über eine Import-Möglichkeit genutzt werden.

In der Perspektive erfolgt die Verwaltung der dienstlichen mobilen Endgeräte, bspw. die auf iOS und Android basieren, durch ein Mobile Device bzw. Enterprise Mobility Management (MDM/EMM). Damit wären abweichende Nutzungsszenarien denkbar.

## 4.2. Organisatorischer Ablauf der Ticketerstellung

Beschäftigte der HSF können für ihr dienstlich bereitgestelltes oder auch privates Endgerät einen WLAN-Zugang beantragen. Dazu ist eine Anforderung von Mitarbeitern und Dozenten als formlose E-Mail an das ZIT bzw. die Studienorganisatoren des eigenen Fachbereichs zu übermitteln und kurz zu begründen. Für private Endgeräte ist darüber hinaus die Nutzung zu dienstlich förderlichen Zwecken gesondert darzustellen.

Bis zum Einsatz des eduroam-WLAN ist die Nutzung des Self-Service-WLAN auch für die Studierenden der HSF zulässig. Die Studenten sammeln über ihre Seminargruppensprecher die Nutzungsanforderungen je Seminargruppe und geben diese als Anforderungs-Liste an die Studentensekretariate. Die Mitarbeiter der Studentensekretariate erstellen die WLAN-Tickets der Studenten und geben diese an die Studenten weiter. Die Studenten selbst haben keinen Zugang zum Serviceportal, um Tickets auszustellen.

Die berechtigten Nutzer rufen zunächst das Web-Portal für die Ticketerstellung (<http://sponsor.zd.sachsen.de>) auf. Die Anmeldung am Portal erfolgt mit dem AD-Benutzeraccount (Anmeldename) und angehängtem @smi.sachsen.de.

Im Feld „Gasttyp“ stehen zwei verschiedene WLAN-Ticket-Typen zur Auswahl. Für die Mitarbeiter und Studenten ist der Eintrag „Gast\_MA\_Selfservice\_180\_Tage“ als WLAN-Zugangsticket zu wählen. Die Tickets werden im Regelfall für 180 Tage ausgestellt, kürzere Zeiträume sind je nach Erfordernis und Entscheidung durch den erstellenden Bearbeiter in Abstimmung mit dem Antragsteller möglich.

Der Erstellungsprozess ist in Anlage 3 detailliert dargestellt.

Die Ticket-Zugangsdaten werden durch den Ersteller auf vertraulichem Wege an den Nutzer weitergegeben. Der Nutzer hat die Möglichkeit, maximal 5 Geräte über dieses Ticket zu registrieren.

## 5. WLAN für Gäste der HSF über das WLAN-Gast-Portal

### 5.1. Einsatzzweck

Der WLAN-Gastzugriff ist für externe Nutzer vorgesehen, welche das Internet über die SVN-Infrastruktur unter Umgehung aller im SVN angebotenen Dienste ungehindert verwenden möchten. Dies trifft insbesondere auf die Fortbildungsteilnehmer am FoBiZ zu (solange diese nicht als Mitarbeiter einer anderen Behörde selbst bereits über Zugangsdaten verfügen). Der WLAN-Gastzugang darf nicht den Landesbediensteten zur Verfügung gestellt werden. Für Landesbedienstete gilt eine andere Richtlinie und es ist ausschließlich der Self-Service-Zugang zu nutzen.

Diese sogenannten Gasttickets dürfen für grundsätzlich maximal 7 Tage ausgestellt werden. Pro Ticket können bis zu 5 Endgeräte bzw. MAC-Adressen freigeschaltet werden (z. B. für Laptop, Smartphone und Tablet eines Gast-Nutzers).

### 5.2. Organisatorischer Ablauf der Ticketerstellung

Gäste und Fortbildungsteilnehmer der HSF können für ihre privaten Endgeräte einen WLAN-Zugang beantragen. Dazu ist eine Anforderung als formlose E-Mail oder mündlich entsprechend nachfolgender Übersicht an den/die zuständigen Bearbeiter zu richten:

| Zugang für             | Erstellung durch   |
|------------------------|--|
| Gäste                  | Zentrale Dienste / Empfang / Sekretariate der Fachbereiche |
| Fortbildungsteilnehmer | ISB/OSB des FoBiZ  |

Die Erstellung und Ausgabe der Tickets erfolgt durch die berechtigten Mitarbeiter (Mitarbeiter Studienorganisation, zentrale Dienste etc.). Diese melden sich zunächst am Web-Portal für die Ticketerstellung (<http://sponsor.zd.sachsen.de>) an. Im Feld „Gasttyp“ ist der Eintrag „Gast\_MA\_Selfservice\_7\_Tage“ als WLAN-Zugangsticket zu wählen. Die Tickets werden im Regelfall für 7 Tage ausgestellt, kürzere Zeiträume sind je nach Erfordernis und Entscheidung durch den erstellenden Bearbeiter in Abstimmung mit dem Antragsteller möglich. Der Erstellungsprozess ist in Anlage 3 detailliert dargestellt. Die Pflichtfelder sind wahrheitsgemäß auszufüllen. Für die Eintragung bei „besuchter Person“ ist der Gastgeber bzw. der Kurs-Organisator einzutragen. Als Gruppen-Bezeichnung ist eine aussagekräftige Bezeichnung als Zuordnung zum Fachbereich/FoBiZ und Seminargruppe/Seminar einzutragen.

Die Ticket-Zugangsdaten werden durch den Bearbeiter auf vertraulichem Wege an den Antragsteller weitergegeben.

## 6. Nutzungsbedingungen und Datenschutz

Bei der Umsetzung der WLAN-Infrastruktur wurde die aktuell gültige Rechtsprechung bzgl. der Störerhaftung und des Datenschutzes berücksichtigt. Insbesondere wurden die Nutzungs- und Datenschutzbedingungen für die WLAN-Gastnutzung angepasst, die von jedem Gast-Nutzer akzeptiert werden müssen. Der aktuelle Stand der Nutzungs- und Datenschutzbedingungen für die WLAN-Gastnutzung ist als Anlage (Anlage 1 und 2) beigefügt. Mit der Nutzung akzeptiert der Nutzer die Nutzungsbedingungen.

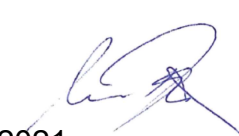
Die WLAN-Zugangsdaten sind personenbezogen und somit nicht an Dritte weiter zu geben.

## 7. Fehlerbehebung

Probleme bei der WLAN-Nutzung sind zunächst mit dem Ersteller des WLAN-Tickets zu klären. Dabei sind folgende Fehler zu prüfen und auszuschließen:

- Übermittlung falscher Zugangsdaten,
- Auswahl des falschen WLAN-Netzes
- falsche Verfahrensweise beim Herstellen der WLAN-Verbindung
- falsche Eingabe der Zugangsdaten,

Sollten die Zugangsprobleme damit noch nicht behoben werden können, ist der Fall an das ZIT über die Hotline 444 abzugeben.



17.02.2021

---

Ullrich Prax

Referent ZIT



27.07.2021

---

Sven Rudolf

Referatsleiter ZIT

# 8. Anhang

## Abkürzungsverzeichnis

| <b>Abkürzung</b> | <b>Bedeutung</b>  |
|------------------|---|
| ACL              | Access Control Liste  |
| AD               | Active Directory  |
| AGB              | Allgemeine Geschäftsbedingungen                               |
| CA               | Certificate Authority   |
| DFN              | Deutsches Forschungsnetz                                      |
| DHCP             | Dynamic Host Configuration Protocol                           |
| DNS              | Domain Name Service   |
| EAP-TLS          | Extensible Authentication Protocol – Transport Layer Security |
| EMM              | Enterprise Mobility Management                                |
| FoBiZ            | Fortbildungszentrum der HSF                                   |
| GPO              | Gruppenrichtlinien-Objekt<br>(group policy object)            |
| HSF              | Hochschule Meißen und Fortbildungszentrum                     |
| IEEE             | Institute of Electrical and Electronics Engineers             |
| IP               | Internet Protocol   |
| LAN              | Local Area Network  |
| MAC              | Media Access Control  |
| MDM              | Mobile Device Management                                      |
| OU               | Organisationseinheit  |
| PoE              | Power over Ethernet   |
| RADIUS           | Remote Authentication Dial-In User Service                    |
| RFC              | Request for Comments  |
| SID              | Sächsische Informatik Dienste                                 |
| SSID             | Service Set Identifier  |
| SVN              | Sächsisches Verwaltungsnetz                                   |
| SVNT             | SVN Terminator (Anschlusseinheit)                             |
| TSI              | T-Systems International                                       |
| VLAN             | Virtual Local Area Network                                    |
| WLAN             | Wireless Local Area Network                                   |
| ZD               | Zentrale Dienste  |
| ZIT              | Zentrum für Informationstechnologie der HSF                   |

## Allgemeine Nutzungsbedingungen für die kostenlose Internetnutzung

Der Freistaat Sachsen, vertreten durch den Geschäftsführer des Staatsbetriebs Sächsische Informatik Dienste, Riesaer Straße 7, 01129 Dresden (nachfolgend auch "wir") bietet Ihnen als externen Nutzer die Möglichkeit, kostenlos und zeitlich begrenzt den Internetzugang über WLAN in den Behörden zu nutzen.

### I. Registrierung

Dem Gast wird durch einen internen Mitarbeiter ein Gast-Account / Ticket per Email bzw. in Papierform zur Verfügung gestellt. Der Account für den Gast wird über ein sogenanntes Gast-Portal erstellt. Die Laufzeiten können dabei entsprechend angepasst werden. Jedoch darf die Laufzeit des Gast-Accounts / Tickets maximal 7 Tage bzw. 180 Tage (je nach Berechtigung) betragen.

### II. WLAN-Nutzung

Der Gast verbindet sein Endgerät mit der WLAN-SSID „SVN-GastNetz“, öffnet einen Internetbrowser mit Angabe einer beliebigen URL und gibt nach Aufforderung im Internetbrowser seine entsprechend dem Gast-Account / Ticket lautenden Daten ein. Danach müssen die WLAN-Vorgaben der Landesverwaltung Sachsen (AGB) akzeptiert werden. Für die Laufzeit des Gast-Accounts / Tickets ist das Endgerät, genauer gesagt eine Netzwerkschnittstelle bzw. MAC-Adresse des Endgeräts, per NAT mit dem Internet verbunden und kann sich darin frei bewegen. Eine Beschränkung von Protokollen bzw. Ports erfolgt nicht.

### III. Sicherheit

Die kabellose Datenübertragung zwischen dem Router und dem WLAN-fähigen Endgerät des Gastes erfolgt unverschlüsselt. Daher kann nicht ausgeschlossen werden, dass sich Dritte unbefugt Zugriff auf die mittels WLAN zu übertragenden Daten verschaffen.

### IV. Pflichten und Obliegenheiten des Gastes

1. Der Internetzugang darf nicht missbräuchlich genutzt werden, insbesondere
  - a. dürfen keine gesetzlich verbotenen, unaufgeforderten Informationen, Sachen und sonstige Leistungen übersandt werden, wie z. B. unerwünschte und unverlangte Werbung per E-Mail oder SMS
  - b. darf keine rechtswidrige Kontaktaufnahme durch Telekommunikationsmittel erfolgen (§ 238 Strafgesetzbuch ("StGB")).
  - c. dürfen keine Informationen mit rechts- oder sittenwidrigen Inhalten übermittelt oder in das Internet eingestellt werden und es darf nicht auf solche Informationen hingewiesen werden. Dazu zählen vor allem Informationen, die im Sinne der §§ 130, 130a und 131 StGB der Volksverhetzung dienen, zu Straftaten anleiten oder Gewalt verherrlichen oder verharmlosen, sexuell anstößig sind, im Sinne des § 184 StGB pornografisch sind, geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden oder in ihrem Wohl zu beeinträchtigen oder das Ansehen des Freistaats Sachsens schädigen können. Die Bestimmungen des Jugendmedienstaatsvertrages und des Jugendschutzgesetzes sind zu beachten.
  - d. ist dafür Sorge zu tragen, dass durch die Inanspruchnahme einzelner Funktionalitäten und insbesondere durch die Einstellung oder das Versenden von Nachrichten keinerlei Beeinträchtigungen für uns, andere Anbieter oder sonstige Dritte entstehen.
  - e. dürfen keine Verbindungen hergestellt werden, die Auszahlungen oder andere Gegenleistungen Dritter an den Gast zur Folge haben.
  - f. sind die nationalen und internationalen Urheber- und Marken-, Patent-, Namens- und Kennzeichenrechte sowie sonstigen gewerblichen Schutzrechte und Persönlichkeitsrechte Dritter zu beachten.
2. Es obliegt dem Gast eine spezielle Sicherheitskonfiguration seiner Software vorzunehmen, damit die Datenübertragung vor Zugriffen Dritter geschützt ist. Eine Verbindung ins Internet ist durch den Gast stets durch „Logout“ zu beenden.

3. Zugangsdaten (wie Benutzername/Passwort) dürfen nicht an Dritte weitergegeben werden und sind vor dem Zugriff durch Dritte geschützt aufzubewahren.
4. Der Freistaat Sachsen und seine Erfüllungsgehilfen sind von sämtlichen Ansprüchen Dritter freizustellen, die auf einer rechtswidrigen Verwendung des Internetzugangs durch den Gast beruhen oder mit seiner Billigung erfolgen oder die sich insbesondere aus datenschutzrechtlichen, urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit der WLAN-Nutzung verbunden sind. Erkennt der Gast oder muss er erkennen, dass ein solcher Verstoß droht, besteht die Pflicht zur unverzüglichen Unterrichtung des Freistaats Sachsen.

## **V. Verantwortung für Inhalte**

Der Gast ist für die Inhalte, welche er über den Internetzugang abrufen, über den Internetzugang einstellt oder die in irgendeiner Weise verbreitet werden, gegenüber dem Freistaat Sachsen und Dritten selbst verantwortlich. Die Inhalte unterliegen keiner Überprüfung durch uns.

## **VI. Beschränkte Leistungs- und Haftpflichten**

1. Wir stellen den Internetzugang freiwillig und unentgeltlich bereit und übernehmen keinerlei Leistungspflichten oder Gewähr, dass der Internetzugang in einem bestimmten Umfang verfügbar ist. Wir haften bei Vorsatz und grober Fahrlässigkeit unbeschränkt für alle von uns (einschließlich der gesetzlichen Vertreter oder Erfüllungsgehilfen) verursachten Schäden.
2. Wir können den kostenlosen Internetzugang jederzeit im Ganzen oder teilweise vorübergehend oder endgültig einstellen oder einschränken. Einzelne Gast-Accounts können insbesondere auch bei Verstoß gegen die Nutzungsbedingungen gesperrt werden.

## **VII. Änderungen der Nutzungsbedingungen**

Die jeweils geltenden Nutzungsbedingungen sind auf unserer Webseite abrufbar und können durch uns geändert werden, soweit dies aus triftigem, bei Zugangsgewährung zum Internet nicht vorhersehbarem Grund, erforderlich ist. Setzen Sie die Nutzung fort, so erklären Sie sich mit geänderten Bedingungen einverstanden.

## Datenschutzbestimmungen

Stand: 28.09.2018

### § 1 Information über die Erhebung personenbezogener Daten gemäß Art. 13 Datenschutzgrundverordnung ("DSGVO")

- (1) Für die in diesen Datenschutzbestimmungen beschriebene Datenverarbeitung ist der Verantwortliche gemäß Art. 4 Abs. 7 DS-GVO:

Freistaat Sachsen  
vertreten durch den Geschäftsführer des Staatsbetriebs Sächsische Informatik  
Dienste

Riesaer Straße 7 (red. Anm. aktuell: Dresdner Straße 78A)

01129 Dresden (red. Anm. aktuell: 01445 Radebeul)

[datenschutz@sid.sachsen.de](mailto:datenschutz@sid.sachsen.de)

(nachfolgend "**wir**").

- (2) Den Datenschutzbeauftragten der Sächsischen Staatskanzlei erreichen Sie unter:

Sächsische Staatskanzlei

Archivstraße 1

01097 Dresden

[datenschutz@sk.sachsen.de](mailto:datenschutz@sk.sachsen.de)

+49 351 564-1185 (red. Anm. aktuell: - 11310)

- (3) Diese Datenschutzzinformation gilt für die Verarbeitung von Daten von Nutzern des Gast-WLANs.

- (4) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

### § 2 Erhebung personenbezogener Daten bei der Nutzung des Gast-WLANs

- (1) Wenn Sie das Gast-WLAN nutzen, erheben wir automatisch die folgenden personenbezogenen Daten, die Sie oder Ihr Gerät an unseren Server übermitteln:

- Vorname,
- Nachname,
- E-Mail-Adresse,
- Telefonnummer,
- Unternehmen,
- Besuchte Person (E-Mail),
- Grund des Besuchs,
- Gruppen-Tag (um den Grund des Besuchs in Untergruppe zu präzisieren),
- Dauer der Nutzungsbefugnis (Tage),
- Startzeitpunkt des Tickets,
- Endzeitpunkt des Tickets,
- Benutzername für WLAN-Gastzugang,
- Kennwort für WLAN-Gastzugang und
- MAC-Adresse des Endgerätes.

### § 3 Zweck der Verarbeitung und Rechtsgrundlage

- (1) Wir verarbeiten diese Daten (i) auf Grundlage eines unentgeltlichen Nutzungsvertrags (Art. 6 Abs. 1 S. 1 lit. b) DS-GVO), um Ihnen unser Gast-WLAN zur ausschließlichen Nutzung des Internets zur Verfügung stellen zu können und (ii) auf Grundlage einer Interessenabwägung, um die Stabilität und Sicherheit unseres Netzwerks zu gewährleisten (Art. 6 Abs. 1 S. 1 lit. f) DS-GVO). Zusätzliche Informationen zur

Interessenabwägung können Sie gerne anfordern, indem Sie uns wie in Ziffer 1 oben angegeben kontaktieren.

- (2) Die Bereitstellung der personenbezogenen Daten ist weder gesetzlich noch vertraglich vorgeschrieben. Jedoch ist die Bereitstellung dieser Daten notwendig, um das Gast-WLAN zu nutzen. Ihnen entstehen aus der Nichtbereitstellung der Daten keine rechtlichen Nachteile.

#### § 4 Aufbewahrung

Wir löschen diese Daten eine Woche nach Ablauf der Nutzungserlaubnis. Die wird entweder für einen Zeitraum von 7 Tagen oder 180 Tagen gewährt.

#### § 5 Empfänger

Für die Zurverfügungstellung des WLAN-Netzes werden wir Ihre personenbezogenen Daten an unseren Telekommunikationspartner T-Systems in Deutschland übermitteln. Jeglicher Zugang zu Ihren personenbezogenen Daten ist beschränkt auf diejenigen Personen, bei denen die Notwendigkeit zur Kenntnisnahme besteht, um deren Tätigkeitsverpflichtung zu erfüllen.

#### § 6 Ihre Rechte

- (1) Sie haben gegenüber uns folgende Rechte hinsichtlich der Verarbeitung der Sie betreffenden personenbezogenen Daten durch uns:

- Recht auf Auskunft (Art. 15 DS-GVO);
- Recht auf Berichtigung (Art. 16 DS-GVO);
- Recht auf Berichtigung oder Löschung (Art. 17 DS-GVO);
- Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO);
- Recht auf Datenübertragbarkeit (Art. 20 DS-GVO);
- Recht auf Widerspruch gegen die Verarbeitung (21 DS-GVO).

- (2) Nachstehend finden Sie weitere Informationen über Ihre Rechte:

**Recht auf Auskunft über Ihre personenbezogenen Daten:** Soweit vom anwendbaren Datenschutzrecht vorgesehen, haben Sie das Recht, von uns eine Bestätigung darüber zu verlangen, ob Ihre personenbezogenen Daten verarbeitet werden oder nicht, und, sofern dies der Fall ist, haben Sie das Recht, Auskunft über diese personenbezogenen Daten zu verlangen. Die Auskunftsinformation umfasst – unter anderem – die Verarbeitungszwecke, die Kategorien der betroffenen personenbezogenen Daten und die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden. Jedoch ist das kein absolutes Recht und die Interessen anderer Personen können Ihr Auskunftsrecht beschränken.

Sie haben außerdem das Recht, eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zu erhalten. Sofern Sie weitere Kopien verlangen, können wir ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.

**Recht auf Berichtigung:** Soweit vom anwendbaren Datenschutzrecht vorgesehen, haben Sie das Recht, von uns Berichtigung unrichtiger personenbezogener Daten, die Sie betreffen, zu verlangen. Abhängig von den Zwecken der Verarbeitung haben Sie das Recht, dass Ihre unvollständigen personenbezogenen Daten vervollständigt werden, auch mittels einer ergänzenden Erklärung.



**Recht auf Löschung (Recht auf Vergessenwerden):** Soweit vom anwendbaren Datenschutzrecht vorgesehen, haben Sie das Recht, von uns die Löschung der Sie betreffenden personenbezogenen Daten zu erwirken und wir können verpflichtet sein, solche personenbezogenen Daten zu löschen.

**Recht auf Einschränkung der Verarbeitung:** Soweit vom anwendbaren Datenschutzrecht vorgesehen, haben Sie das Recht, von uns die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen. Wir können auch verpflichtet sein, die Verarbeitung Ihrer personenbezogenen Daten einzuschränken. In diesem Fall werden die betroffenen personenbezogenen Daten gekennzeichnet und dürfen von uns nur für bestimmte Zwecke verarbeitet werden.

**Recht auf Datenübertragbarkeit:** Soweit vom anwendbaren Datenschutzrecht vorgesehen, haben Sie das Recht, Sie betreffende personenbezogene Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und Sie haben das Recht, diese personenbezogenen Daten ohne Behinderung unsererseits zu einer anderen Einheit zu übertragen, sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt und auf einer Einwilligung gemäß Art. 6 Abs. 1 lit. a DS-GVO bzw. auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b DS-GVO beruht.

**Widerspruchsrecht:** Unter bestimmten Umständen haben Sie das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten zu erheben, und wir sind verpflichtet, Ihre personenbezogenen Daten nicht länger zu verarbeiten. Falls Sie ein Widerspruchsrecht haben und falls Sie dieses Recht ausüben, werden Ihre personenbezogenen Daten nicht mehr für diese Zwecke von uns verarbeitet. Sie können dieses Recht ausüben, indem Sie uns wie in Ziffer 7 unten angegeben kontaktieren. Ein solches Widerspruchsrecht kann insbesondere dann nicht vorliegen, wenn die Verarbeitung Ihrer personenbezogenen Daten notwendig ist, um mit Ihnen einen Vertrag durchzuführen.

- (3) Bitte beachten Sie, dass das Recht auf Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie das Recht, der Verarbeitung zu widersprechen, nur unter bestimmten weiteren rechtlichen Voraussetzungen besteht. Für das Auskunftsrecht gelten die Einschränkungen nach § 34 BDSG.
- (4) Sie haben zudem das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über die Verarbeitung Ihrer personenbezogenen Daten durch uns zu beschweren.