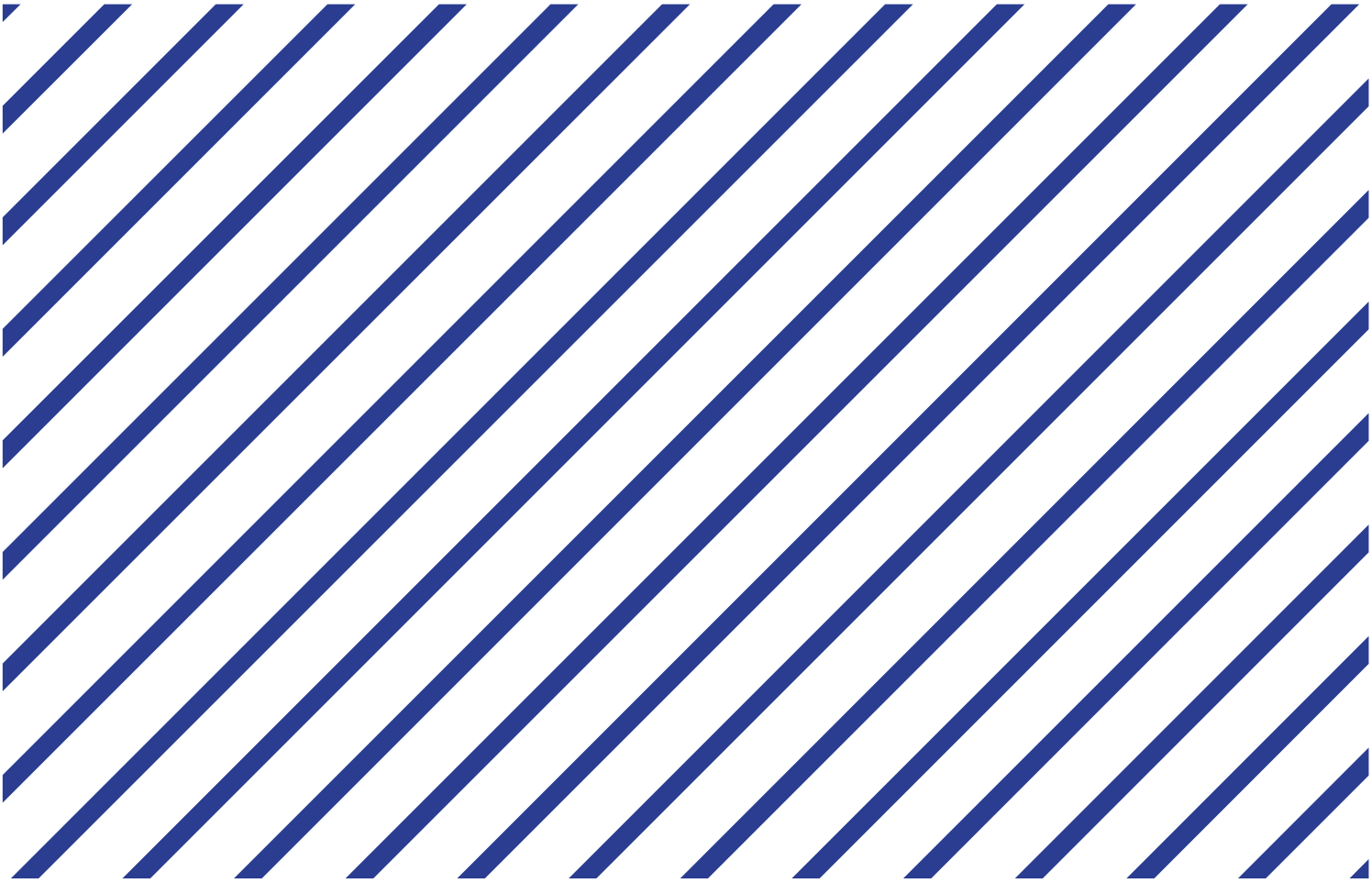

FH MÜNSTER
University of Applied Sciences

Betriebskonzept zur WLAN SSID „IoT-Lab“

Stand: 10.12.2020 (Version 1.3)

Inhaltsverzeichnis

1. Allgemeines

Immer mehr Messsysteme besitzen die Fähigkeit mittels WLAN-Verbindungen Messdaten kabellos an entsprechende Auswertungssysteme zu senden. Dies stellt an die Infrastruktur des Netzbetreibers zusätzliche Anforderungen, welche geplant und umgesetzt werden müssen. Zudem kommt noch der Sicherheitsaspekt, dass die Messdaten sensitive Daten enthalten können und somit besonders schützenswert sind.

Die Problematik besteht in der Anbindung der Messsysteme, da diese oft nicht den personalisierten Authentifizierungsprozess unterstützen. Daher ist es erforderlich, Rahmenbedingungen für den Betrieb eines solchen Netzes zu definieren.

Im Nachfolgenden werden diese Rahmenbedingungen schriftlich festgehalten. Die Rahmenbedingungen können Änderungen unterliegen, um den technischen Anforderungen des Netzbetreibers gerecht zu werden.

Die FH-Münster stellt für kabellose Messsysteme ab sofort folgende WLAN SSID zur Verfügung:

IoT-Lab

Diese WLAN SSID steht allen Fachbereichen zur Verfügung.

2. Anmeldung

Der Zugriff dieser SSID ist streng reglementiert. Jedes Messsystem ist mit seiner Physikalischen WLAN MAC-Adresse bei der Datenverarbeitungszentrale (DVZ) anzumelden. Systeme, welche nicht bei der DVZ angemeldet sind, wird der Zugriff verwehrt. Bei der Ausmusterung alter Messsysteme, sind diese wieder bei der DVZ abzumelden. Für die Anmeldung ist die Geräteregistrierung im myFH-Portal unter „Meine IT-Dienste“ zu verwenden. Eine **Anleitung** wird im Wiki der Datenverarbeitungs-zentrale bereitgestellt.

3. Zugriffsbeschränkungen

Das IoT-WLAN ist auf den Zugriff auf folgende hochschulinterne Ressourcen beschränkt:

- DHCP/DNS Server
- Speziell freigeschaltete, hausinterne Rechensysteme, zu denen die Messdaten übermittelt werden

Die IP-Adressen der hausinternen Rechensysteme sind vom jeweiligen Nutzer bei der DVZ anzugeben. Alle weiteren Verbindungen, auch der Internetzugriff, sind nicht gestattet.

Für Updates/Wartungsarbeiten der Messsysteme ist der Nutzer selbst verantwortlich.

Die Kommunikation innerhalb der SSID wird nicht beschränkt. Für den etwaigen Schutz gegenüber anderen Systemen ist der Systembetreiber zuständig.

4. Ausstrahlung

Die WLAN SSID „IoT-Lab“ wird nur an den Standorten ausgestrahlt, an welchen sie benötigt wird und an denen sie keine Beeinträchtigung auf die SSID „eduroam“ ausübt.

Eine Ausleuchtung von Außenbereichen ist nicht vorgesehen.

Ein separater WLAN Ausbau für die SSID „IoT-Lab“ ist nicht vorgesehen.

5. Wartung und Ausfall

Die DVZ wird die Wartung mit den Standards der SSID „eduroam“ gleichsetzen. Im Falle einer Wartung oder eines Ausfalls des WLAN Controllers, wird der Backup WLAN Controller die SSID weiterverwalten. Dabei stehen die ursprünglich vergebenen IP-Adressen bis zur Beendigung der Wartungsarbeiten nicht zur Verfügung.

6. Sicherheit

Die WLAN SSID wird mit einem Pre-shared Key (PSK) abgesichert. Der PSK verwendet eine WPA2 Verschlüsselung. Außerdem wird eine Access-Control-List (ACL) auf dem WLAN Controller geführt, welche nur angemeldete Systeme zur Authentifizierung zulässt.

Der Pre-shared Key wird an den Nutzer bei Einverständnis mit diesem Betriebskonzept übergeben und ist nur für IoT Systeme vorgesehen. Er ist vom Nutzer geheim zu halten und nicht an Dritte weiterzugeben.

Die DVZ behält sich das Recht vor, den Pre-shared Key zu ändern. Dieser wird in einem solchen Fall an die entsprechenden Nutzer weiter gegeben.