

„Migration - Amman“



Version: 1.0

Thema: Migration

Vorgelegt von

Daniel Palumbo

Projektleiter:

Herr Schaad

Pratteln, September 2023

Management Summary

|  |
| --- |
| * **Wo stehen wir heute**   Das Projekt wird von der «Just Relax ICT» übernommen da die Firma Konkurs ging. Deshalb haben wir, die Firma «Palumbo IT GmbH», das Projekt. Hauptaugenmerk liegt dabei bei der schon angefangenen Migration auf eine modernere IT-Lösung, da die aktuell vorhandene Lösung, nicht mehr den Ansprüchen des Kunden nicht gerecht wird.  Die Garage Ammann ist ein Betrieb mit 16 Mitarbeiter, sie reparieren und verkaufen Fahrzeuge. Dies schon bereits in der 3. Generation.   * **Was ändert das neue Produkt/Projekt**   In Kapitel 3-Vorgehensplanung sind alle Änderungen protokolliert.   * **Wie lange dauert die Änderung/Implementierung**   Die Implementierung wird etwa eine Woche in Anspruch nehmen.   * **Wie viel wird das Projekt im Total kosten**   Die genauen Kosten sind im Moment noch nicht ersichtlich. Diese werden während der Aufarbeitung evaluiert. |

Dokumentenmanagement

Version/Status: Siehe Tabelle unten

Datum: 03.09.2023

Autoren: Daniel Palumbo (DP)

Dateiname:

Änderungsgeschichte

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vers.** | **Datum** | **Autoren** | **Status** | **Änderung** |
| 0.1 | 01.09.2023 | DP | Initial | - Dokument erstellt |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Inhaltsverzeichnis

[Inhaltsverzeichnis 3](#_Toc144654793)

[1 Ausgangslage 4](#_Toc144654794)

[1.1 Aktueller Netzwerkplan 4](#_Toc144654795)

[2 Vorgehensplanung 5](#_Toc144654796)

[3 Konzepte 7](#_Toc144654797)

[3.1 Namenskonzept 7](#_Toc144654798)

[3.2 Gruppen- und Benutzerkonzept 8](#_Toc144654799)

[3.3 Benutzerkonzept 8](#_Toc144654800)

[3.4 Sicherheitsgruppenkonzept 8](#_Toc144654801)

[3.5 Gruppenkonzept 8](#_Toc144654802)

[3.6 Gruppenverschachtelung 9](#_Toc144654803)

[3.7 IP-Adresskonzept 9](#_Toc144654804)

[4 Dokumentation 10](#_Toc144654805)

[4.1 Basis Kennwörter 10](#_Toc144654806)

[4.2 IP-Adressliste / Hostnameliste 10](#_Toc144654807)

[4.3 BIOS-Einstellungen 10](#_Toc144654808)

[4.4 DNS-Einstellungen 10](#_Toc144654809)

[4.5 DHCP-Einstellungen 11](#_Toc144654810)

[4.6 Gruppen-Liste 11](#_Toc144654811)

[4.7 Sicherheitsgruppen-Liste 11](#_Toc144654812)

[4.8 Freigaben-Liste 12](#_Toc144654813)

[4.9 Benutzer-Liste 12](#_Toc144654814)

[4.10 Geräte-Liste und Konfiguration 13](#_Toc144654815)

[4.10.1 Physischer ESXi Server (MW-WAN-SRV-01) 13](#_Toc144654816)

[4.10.2 13](#_Toc144654817)

[4.10.3 VM Windows Server 19 (MW-WAN-SRV-02) 13](#_Toc144654818)

[4.10.4 13](#_Toc144654819)

[4.10.5 VM Windows 10 (MW-WAN-WOR-01) 14](#_Toc144654820)

[4.10.6 14](#_Toc144654821)

[4.11 Datenerhebungsformular 15](#_Toc144654822)

[5 Selbstständigkeitserklärung 16](#_Toc144654823)

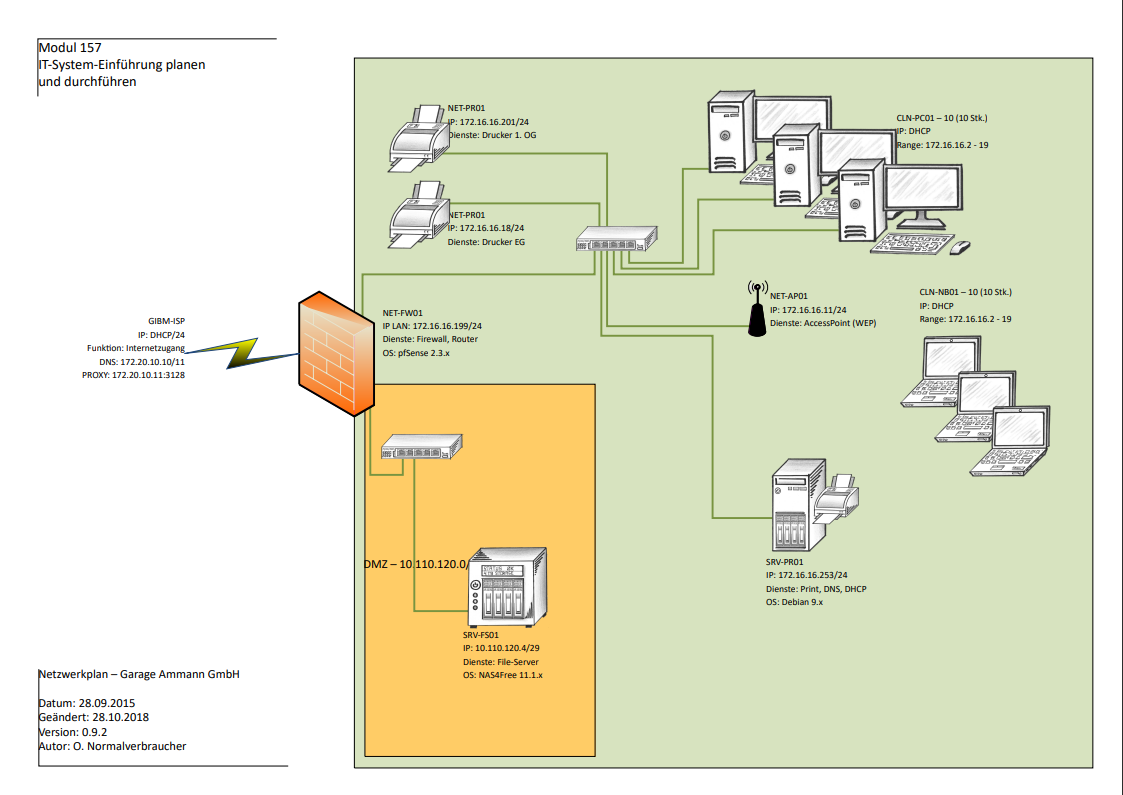
[6 Quellen 17](#_Toc144654824)

# Ausgangslage

Die Migration ist eine nicht ganz normale, diese wird nämlich wesentlich erschwert, da der alte IT-Dienstleister, die Dokumentation nicht fertigstellen konnte. So werden wir als erstes die Dokumentation fertigstellen und diverse Anpassungen vornehmen. Der Ablauf des Projektes wird in der Terminplanung genauer definiert. Die wichtigsten Punkte des Projektes beinhalten folgendes: Planung, Testen, Umsetzung Testphase und zu guter Letzt der Projektabschluss.

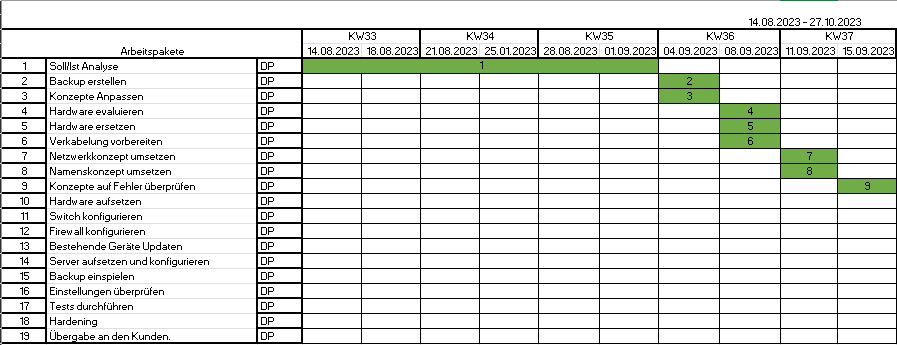
## Aktueller Netzwerkplan

Der aktuelle Netzwerkplan der noch von der Firma «Just Relax ICT» bereitgestellt wurde.



## Terminplanung

So stellen wir uns den Ablauf der Arbeiten vor.



Ein Bild, das Text, Quadrat, Reihe, Screenshot enthält.

Automatisch generierte Beschreibung

Detailierter zu sehen in dem Beigefügtem Dokument «Terminplanung\_Palumbo».

# Vorgehensplanung

|  |  |  |
| --- | --- | --- |
| **Ist-Situation** | **Soll-Situation** | **Machbarkeit** |
| IP-Konzept ist teilweise umgesetzt. | IP-Konzept wurde überarbeitet und umgesetzt. | IP-Konzept gemäss diesem Dokument anpassen. Server und Clients müssen dafür auf ihre IP überprüft werden. |
| Namenskonzept ist teilweise umgesetzt. | Namenskonzept wurde überarbeitet und umgesetzt. | Das Namenskonzept auf alle Geräte, Benutzer und Gruppen gemäss diesem Dokument anwenden. |
| Backup Konzept ist vorhanden. | Backup Konzept wird angepasst und gemäss diesem Dokument verbessert. | Backup Konzept überarbeiten und danach einführen. |
| Bestehendes NAS ist in der DMZ. | Nas im LAN mit neuem OS. | Vorhandenen NAS aus der DMZ in das LAN wechseln und mit FreeNAS aufsetzen. |
| Veraltete Hardware | Auf aktuelle Hardware umrüsten. | Hardware durchgehen und gegebenenfalls austauschen, wenn diese nicht mehr dem aktuellen Standard entspricht. |
| Netzwerke zum Teil aufgesetzt. | Netzwerke wie WAN, LAN und DMZ sind konfiguriert. | Netzwerke sind nach dem Konzept dieses Dokuments zu konfigurieren. |
| DHCP-Range vorhanden. | DHCP-Range angepasst. | DHCP-Range nach diesem Konzept umsetzen. |
| Firewall nicht optimal konfiguriert. | Firewall sicher konfiguriert. | Firewall nach diesem Konzept umsetzen, Regeln wie Any to Any sind ein Nogo. |
| Zugrisskonzept vorhanden. | Zugriffskonzept überarbeitet. | Zugriffskonzept überarbeiten gemäss diesem Dokument. |
| Keine Zentrale Benutzerverwaltung | Active Directory ist vorhanden und konfiguriert. | Auf dem Windows Server wird ein Active-Directory installiert und gemäss Benutzerliste und Gruppenliste konfiguriert. |
| Gruppenkonzept nicht vollständig | Gruppenkonzept überarbeitet. | Gruppenkonzept gemäss diesem Dokument erstellt. |
| Firewall ist veraltet | Firewall ist auf dem neuesten Stand. | Firewall Software aktualisieren, Hardware kann bestehen bleiben. |
| Clients laufen mit alter OS-Version | Clients laufen mit aktueller OS-Version: | Clients auf das aktuelle Betriebssystem aktualisieren. |
| Switch vorhanden | Aktueller Switch mit POE. | Switch mit einem Modell tauschen, welcher auch POE-Unterstützt. |
| Access Point vorhanden. | Neuer Access Point mit POE | Access Point mit einem Modell ersetzen, welches mit POE betrieben werden kann. |
| Netzwerkplan teilweise vorhanden. | Netzwerkplan aktualisert. | Netzwerkplan neu erstellt mit aktuellen Daten. |

# Konzepte

## Namenskonzept

Das Namenskonzept gibt vor, wie sich die Hostnamen zusammensetzen und nach welchen Richtlinien diese Kennung zusammengestellt wird.

* Firmenkürzel: 2 Zeichen
* Standort: 2 Zeichen
* Systeme: 3 Zeichen
* Nummerierung: 2 Zahlen (Vorlaufen)

#### Firmenkürzel

|  |  |
| --- | --- |
| Firmenkürzel | Beschreibung |
| GA | Garage Amman |

#### Systeme

|  |  |
| --- | --- |
| Kürzel | Beschreibung |
| SRV | Server |
| ROU | Router |
| STO | Storage |
| PRI | Printer |
| WOR | Workstation |
| HST | Host |

#### Standorte

|  |  |
| --- | --- |
| Kürzel | Beschreibung |
| BSL | Basel |

#### Domain

m157.intra

#### Syntax

{ Firmenkürzel (2) } - { Standort (2) } – { Systeme (3) } – { 2-stellige Nummer (2) }

## Gruppen- und Benutzerkonzept

## Benutzerkonzept

* Benutzernamen werden aus dem ersten Buchstaben des Vornamen und dem ganzen Nachnamen, getrennt von einem Punkt gebildet.
* Umlaute werden mit UE,AE etc. geschrieben.
* Sonderzeichen wie „èà“ usw. werden als „ea“ geschrieben.
* Doppelte Namen werden mit einer Nummerierung ergänzt.
* Aus dem Benutzernamen wird auch gleich die Email gebildet.

#### Syntax

{ v }.{ nachname }

## Sicherheitsgruppenkonzept

* Gruppennamen werden gleich der Abteilung/des Teams benannt.
* Doppelte Gruppen sind nicht erlaubt.
* Sonderzeichen wie „èà“ usw. werden als „ea“ geschrieben.

#### Syntax

{ Gruppenname }

## Gruppenkonzept

* Gruppennamen werden gleich der Abteilung/des Teams benannt. Davor steht ein „P\_“ für Permission und dahinter ein z.b. „\_r“ (read)
* Doppelte Gruppen sind nicht erlaubt.
* Sonderzeichen wie „èà“ usw. werden als „ea“ geschrieben.

#### Syntax

{P}\_{Gruppenname]\_{Berechtigung}

**Legende: r = lesen (read) w = schreiben (write) x = lesen/ausführen (execute)**

## Gruppenverschachtelung

**A-G-DL-P bedeutet, dass die Berechtigungen nach einer bestimmten Methode vergeben werden:**

* **A**= Account, der Mitglied einer
* **G**= Globalen Gruppe ist, die alle User einer bestimmten Abteilung enthält, welche wiederum Mitglieder einer
* **DL**= Domänenlokalen Gruppe sind, die speziell für eine bestimmte Berechtigung erstellt wurde und deshalb in der
* **P**= Permission (ACL) eines Verzeichnisses eingetragen ist.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | 🡪 | Abteilungs-Gruppe | 🡪 | Berechtigungs-Gruppe |
| H.Meiser | 🡪 | Einkauf | 🡪 | P\_Verkauf\_R / P\_Einkauf\_M |
|  | 🡪 |  | 🡪 |  |

## IP-Adresskonzept

In unserem physikalischen Netzwerk befinden sich verschiedene IP-Adressierungssegmente. Dieser Installation steht ein 24er Subnetz zur Verfügung, welches jedoch in einem 16er Subnetz genutzt wird.

Top-Level IP Adressierung (16er Subnetz). (XX.XX.XXX.XXX)

|  |  |
| --- | --- |
| IP Bereich | Funktion und Beschreibung |
| 001 – 009 | Netzwergeräte (Eigene Gateway,Switch, etc.) |
| 010 – 019 | Physikale Server (Hosts) |
| 020 – 029 | VM Server |
| 030 – 039 | Storage |
| 040 – 049 | Drucker |
| 050 – 069 | Reserve |
| 070 – 099 | Test VM und VM Workstation |
| 100 – 199 | DHCP Bereich |
| 200 - 254 | Reserve |

# Dokumentation

## Basis Kennwörter

|  |  |  |  |
| --- | --- | --- | --- |
| System | Funktion | Benutzer | Kennwort |
| ESXi Host | Hauptbenutzer (Administrator) | root | P+ssw0rd |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## IP-Adressliste / Hostnameliste

#### Top Level IP Adressen (vorgaben ILV)

Gateway: **XXX.XX.X.XX**

DNS ILV: **XXX.XX.X.XX**

#### LAN Subnetz

IP-Subnetz: **XX.XX.XXX.0 / 24**

|  |  |  |  |
| --- | --- | --- | --- |
| System | Hostname | IP Adresse | Netzwerk |
| ESXi Host | MW-WAN-SRV-01 | 172.17.211.10 | LAN |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### Domän-Name

**MW.ICTW** *(NetBios-Name: MW)*

## BIOS-Einstellungen

|  |  |
| --- | --- |
| Einstellung | Wert |
| Load Defaults Settings | **Yes** |
| Boot Mode Select | **Legacy** |
| Virtualization | **Enable** |

## DNS-Einstellungen

|  |  |  |
| --- | --- | --- |
| Konfigurations-Typ | Beschreibung | Konfiguration |
| A-Record | A-Record für XX | XXX.XX.XXX.XX |
|  |  |  |
|  |  |  |
|  |  |  |

## DHCP-Einstellungen

|  |  |  |
| --- | --- | --- |
| Konfigurations-Typ | Beschreibung | Konfiguration |
| DHCP-Range | Verteilbare IPs | 172.17.211.100 - 199 |
| Domain | Vollständer Domain-Name | m157.intra |
| NetBiosname | z.B. benutzt bei der Anmeldung | M157 |
| Router | Standardgateway | xxx.xx.x.xx |

## Gruppen-Liste

|  |  |
| --- | --- |
| Gruppennamen | Beschreibung |
| Einkauf | **Abteilung Einkauf** |
|  |  |
|  |  |
|  |  |

## Sicherheitsgruppen-Liste

|  |  |
| --- | --- |
| Gruppennamen | Beschreibung |
| P\_Einkauf\_M | **Modify-Berechtigung für Freigaben** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Freigaben-Liste

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | Sicherheitsgruppe | | | | |
| Buchstabe | **GruppenName** | **Freigabe** | **Einkauf** | **Verkauf** | **Produktion** | **Administration** | **Reserve** |
| E | Einkauf | \\MW-WAN-SRV-02\abteilungen\einkauf | M | R |  |  |  |
| V | Verkauf | \\MW-WAN-SRV-02\abteilungen\verkauf | R | M |  |  |  |
| P | Produktion | \\MW-WAN-SRV-02\abteilungen\produktion | R | R | M |  |  |
| I | Administration | \\MW-WAN-SRV-02\abteilungen\administration | R | R | R | M |  |
| H | Benutzer | \\MW-WAN-SRV-02\users\homes\%username% |  |  |  |  |  |
| G | Gruppenlaufwerk | \\MW-WAN-SRV-02\Abteilung\gruppenlaufwerk |  |  |  |  |  |

Netzlaufwerke werden anhand der Benutzergruppen gebildet. Ebenso werden die Berechtigungen anhand der Sicherheitsgruppen verteilt.

**Legende: r = lesen (read) m = ändern (modify)**

## Benutzer-Liste

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Benutzername | Vollständiger Name | Aktiv | Passwort | Einkauf | Verkauf | Produktion | Administration | Reserve |
| Administrator | Administrator | Ja | P+ssw0rd |  |  |  |  |  |
| H.Meiser | Hans Meiser | Ja | P+ssw0rd | X |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## Geräte-Liste und Konfiguration

### Physischer ESXi Server (MW-WAN-SRV-01)

|  |  |
| --- | --- |
| DAPA-SRV-01 | ESXi Server |
| Host-Typ | ESXi Host |
| Domäne | M157.intra |
| CPU |  |
| RAM |  |
| Grafikkarte |  |
| Harddisk |  |
| Bildschirm |  |
| MAC |  |
| IP | Siehe IP-Adressliste |

### 

|  |  |  |
| --- | --- | --- |
| Konfigurations-Typ | Beschreibung | Konfiguration |
| Hostname | Name des Hosts | Gemäss Adressliste / Namensliste |
| IP Adresse | Adressierung des Hosts | Gemäss Adressliste / Namensliste |
| NTP Startart | Wie wird der Dienst gestartet | Autostart mit Host |
| NTP Dienst | Server zur Zeitsynchronisierung | 0.ch.pool.ntp.org |
| Lokaler Speicher | Lokaler Speicher zur Installation | 70 GB |

### VM Windows Server 19 (MW-WAN-SRV-02)

|  |  |
| --- | --- |
| DAPA-SRV-02 | Windows-Server-2019 |
| Host-Typ |  |
| Domäne | M157.intra |
| CPU |  |
| RAM |  |
| MAC |  |
| Hardware |  |

### 

|  |  |  |
| --- | --- | --- |
| Konfigurations-Typ | Beschreibung | Konfiguration |
| Hostname | Name des Hosts | Gemäss Adressliste / Namensliste |
| IP Adresse | Adressierung des Hosts | Gemäss Adressliste / Namensliste |
| NTP Startart | Wie wird der Dienst gestartet | Autostart mit Host |
| NTP Dienst | Server zur Zeitsynchronisierung | Bezieht Zeit von MW-WAN-SRV-02 |
| Lokaler Speicher | Lokaler Speicher zur Installation | 70 GB |
| Remote | Remote Desktop | Remote Desktop erlauben |
| Zusätz. Speicher | Neue Partition (z.b. Daten) | Mit Thin provising (Abhängig) |

### VM Windows 10 (MW-WAN-WOR-01)

|  |  |
| --- | --- |
| DAPA-WOR-01 | Windows 10 |
| Host-Typ | ESXi Host |
| Domäne | M157.intra |
| CPU |  |
| RAM |  |
| MAC |  |
| Hardware |  |

### 

|  |  |  |
| --- | --- | --- |
| Konfigurations-Typ | Beschreibung | Konfiguration |
| Hostname | Name des Hosts | Gemäss Adressliste / Namensliste |
| IP Adresse | Adressierung des Hosts | Gemäss Adressliste / Namensliste |
| NTP Startart | Wie wird der Dienst gestartet | Autostart mit Host |
| NTP Dienst | Server zur Zeitsynchronisierung | Bezieht Zeit von MW-WAN-SRV-02 |
| Lokaler Speicher | Lokaler Speicher zur Installation | 70 GB |
| Remote | Remote Desktop | Remote Desktop erlauben |

## Datenerhebungsformular

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Daten** | | | | | | |
| **Nr.** | **Speicherort** | **Daten** | **Verfügbarkeits-anforderungen** | **Heutige Grösse** | **Wachstum pro Jahr** | **Archivierung** |
| 1 | C:\Eigene Dateien\Dokumente\Daniel | Wichtige Dokumente | Immer verfügbar  2-4 Stunden  1 Tag  2 Tage oder mehr |  |  | Nein  Ja, Dauer … Jahre |
| 2 | C:\Eigene Dateien\Dokumente | Alle Dokumente | Immer verfügbar  2-4 Stunden  1 Tag  2 Tage oder mehr |  |  | Nein  Ja, Dauer … Jahre |
| 3 | D:\Bilder | Alle Bilddateien | Immer verfügbar  2-4 Stunden  1 Tag  2 Tage oder mehr |  |  | Nein  Ja, Dauer … Jahre |
| 4 | D:\Videos | Alle Videodateien | Immer verfügbar  2-4 Stunden  1 Tag  2 Tage oder mehr |  |  | Nein  Ja, Dauer … Jahre |
| **Priorität (Reihenfolge der Nr.)** | | | | | | |

*«Datenerhebungsformular gemäss vom Buch «Modul 143: Backup- und Restore-Systeme implementieren»*

# Selbstständigkeitserklärung

Ich erkläre hiermit, dass es sich bei der von mir eingereichten schriftlichen Arbeit mit dem Titel

***Migration Amman***

um eine von mir selbst und ohne unerlaubte Beihilfe sowie in eigenen Worten verfasste Originalarbeit handelt.

Ich bestätige überdies, dass die Arbeit als Ganzes oder in Teilen noch nie zur Bewertung einer anderen schulischen Leistung an der BBZBL oder an einer anderen Ausbildungseinrichtung verwendet wurde.

Verwendung von Quellen und Sekundärliteratur

Ich erkläre weiterhin, dass ich sämtliche in der eingereichten Arbeit enthaltenen Bezüge auf Quellen und Sekundärliteratur als solche kenntlich gemacht habe. Insbesondere bestätige ich, dass ich ausnahmslos und nach bestem Wissen sowohl bei wörtlich übernommenen Aussagen (Zitaten) als auch bei in eigenen Worten wiedergegebenen Aussagen anderer Autorinnen oder Autoren (Paraphrasen) die Urheberschaft angegeben habe.

Sanktionen

Ich nehme zur Kenntnis, dass Arbeiten, welche die Grundsätze der Selbstständigkeitserklärung verletzen – insbesondere solche, die Zitate oder Paraphrasen ohne Herkunftsangaben enthalten –, als Plagiat betrachtet werden und entsprechende rechtliche und disziplinarische Konsequenzen nach sich ziehen können.

Ich bestätige mit meiner Unterschrift die Richtigkeit dieser Angaben.

Autor

Name: Palumbo

Vorname: Daniel

Datum: 01.09.2023

Unterschrift: Ein Bild, das Text, Projektor, Nachthimmel enthält.

Automatisch generierte Beschreibung

# Quellen