# Datensicherungskonzept


BASEL LANDSCHAFT

BILDUNGS-, KULTUR- UND SPORTDIREKTION
BERUFSBILDUNGSZENTRUM BASELLAND

Version: 1.0
Thema: Datensicherungskonzept

Vorgelegt von: Yannick Morgenthaler

Projektleiter: Alexio Moreno

Pratteln, März 2022

# 1 Dokumentenmanagement

| | |
|---|---|
| Version/Status | Siehe Tabelle unten |
| Datum: | 22.03.2022 |
| Autoren: | Yannick Morgenthaler (YM) |
| Dateiname: | 301-Skype-Endbenutzer-V0.2.docx |

Änderungsgeschichte

| Vers. | Datum | Autoren | Status | Änderung |
|---|---|---|---|---|
| 0.1 | 22.03.2022 | YM | Initial | |
| 0.2 | 22.03.2022 | YM | Immer nachführen | Inhaltsverzeichnis |
| 0.7 | 22.03.2022 | YM | Erledigt | Inhalt generieren |
| 0.9 | 22.03.2022 | YM | In Bearbeitung | Formatierung |
| 1.0 | 22.03.2022 | YM | Erledigt | Deckblatt |

# 2 Management Summary

## 2.1 IST

Die Daten werden aktuell nicht gesichert. Es bestehen teilweise Sicherheitskopien auf einer externen Festplatte, doch dies wird nicht zuverlässig durchgeführt. Es wäre unter Umständen noch Hardware vorhanden, um ein DIY NAS zu bauen.

## 2.2 SOLL

Die Daten sollen auf einem NAS gesichert werden. Darunter zählen die Bilder aus der Hobbyfotografie und weitere wichtige Dateien wie elektronisch gesicherte Belege oder andere vertrauliche Dokumente. Der freigegebene Ordner auf dem NAS soll ein das Windows System eingebunden werden. So sind die Daten immer verfügbar und können auch von anderen Geräten im Netzwerk abgerufen werden. Eine Standortredundanz wird durch einen zweiten Standort bei meinem Vater in Basel umgesetzt. Da wird ein zweites NAS aufgesetzt und wird per VPN angesteuert. Es werden keine externen Tools und keine Clouddienste genutzt, da bei dieser Datenmenge fortlaufende Kosten anfallen. Es wird mit einer Datenmenge von rund 6TB gerechnet. Die automatische Synchronisation der beiden NAS wird durch ein Skript auf einem mini PC alle 24h ausgeführt. Um eine Redundanz der Synchronisation zu bieten, wird an beiden Standorten ein VPN Endknoten installiert und auch ein Synchronisations-PC.

Für allgemeine Arbeitsdokumente wird dann doch auf ein Clouddienst gesetzt. Der genutzte Dienst wird GitHub sein. So sind die Daten überall verfügbar und das Home Netzwerk wird keinen Risiken ausgesetzt. Mit diesem Clouddienst sind die Daten auch immer noch Lokal auf den Rechnern abgespeichert und bietet so eine weitere Redundanz.

## 2.3 Aufwand

Der Aufwand besteht lediglich darin die beiden NAS aufzusetzen und den VPN Server in betrieb zu nehmen. Der Zeitaufwand beträgt bis zu 4h.

## 2.4 Kosten

Die Kosten belaufen sich für das benötigte Material auf bis zu 2‘100CHF.

# 3 Inhaltsverzeichnis

# 4 Zu sichernde Daten Bestimmen

Hier werden die Speicherorte aufgezeigt, welche Daten gespeichert werden und wie die Restorezeit aussieht.

## 4.1 IST

Die Dateien werden aktuell nicht regelmässig gesichert und unzuverlässig aktualisiert. Für Schuldateien kommt jedoch jetzt schon GitHub zum einsatz.

| Beschreibung | Kapazität | Gespeicherte Daten | Im Einsatz |
|---|---|---|---|
| Externe Festplatte | 2TB | Alles was wichtig sein könnte und mobil sein muss. | Wird mittlerweile selten genutzt da das Notebook immer dabei ist. |
| GitHub | Unbrgrenzt (Dateigrösse max. 100MB) | Alle Schulsachen sowie selbst geschriebene Programme und Skripts | Wird Täglich genutzt und aktualisiert. |
| Weitere Datenträger wie Festplatten und USB-Sticks | Insgesamt bis zu 24TB | Keine | Werden nie genutzt aufgrund von Alter, Geschwindigkeit, Kapazität, etc. |

Zu sichernde Daten Bestimmen

## 4.2 SOLL

| **Daten** | | | | | | |
|---|---|---|---|---|---|---|
| **Speicherort** | **Daten** | **Backup** | **Verfügbarkeit (benötigte Restore Zeit)** | **Grösse** | **Wachstum / Jahr** | **Archivierung** |
| NAS | Videomaterial<br>Bilder<br>Dokumente welche nicht sofort benötigt werden<br>ISO Dateien von System Backups<br>Installationsmedien | Bei jeder Aktualisierung und Änderung | Innerhalb von wenigen Stunden (Standort und Situationsabhängig) | 6TB | Mind. 500GB | Nein |
| GitHub | Hoch verfügbare Daten | Nach jeder Änderung | Immer wenn Internet vorhanden ist. Dann innerhalb von Sekunden | 5GB | 1GB | Ja<br>Werden erst bei Speicherplatzknappheit gelöscht und mindestens 10 Jahre aufbewahrt. |
| Redundanz NAS | Sicherheitskopie von Core NAS<br>Eine Versions sicherung. | Alle 24h | Innerhalb von wenigen Stunden (Standort und Situationsabhängig) | 12TB | 600GB | Nein |
| Keines | Programme oder ähnliches | | | | | |

## 4.3 Umgang mit streng vertraulichen Daten

Streng vertrauliche Daten werden auf einer Externen Festplatte und einem USB-Stick gespeichert und in einem Safe aufbewahrt.

## 4.4 Reihenfolge der Wiederherstellung

### 4.4.1 Beschädigter Datenträger im PC

Bei einem Beschädigten Datenträger im PC werden die Daten vom NAS im entsprechenden Ordner wieder hergestellt.

### 4.4.2 Beschädigter Datenträger im NAS

Bei einem Beschädigten Datenträger im NAS wird dieser schnellstmöglich ersetzt. Das NAS sollte die verlorenen Daten auf dem Datenträger mittels einer Raidkonfiguration automatisch wieder herstellen können. Ansonsten werden die Daten vom Redundanz-NAS wieder hergestellt.

### 4.4.3 Worstcase PC

Der PC ist endgültig tot. Dann wird der PC mit dem letztverfügbaren Image wieder aufgesetzt und synchronisiert. Sollte das Image beschädigt sein aufgrund einer nicht sauberen Kopie, dann wird der PC wie ein neuer PC aufgesetzt, um allfällige Fehler im System zu vermeiden.

### 4.4.4 Worstcase NAS

Ein NAS ist tot. Zuerst folgt eine Fehleranalyse. Sollte das NAS einen Hardwaredefekt erlitten haben, dann wird das entsprechende Teil ersetzt. Sollten aber alle Festplatten auf einmal nicht mehr funktionieren aufgrund verschiedener Gründe, dann können die Daten vom Redundanz-NAS oder vom Core-NAS wiederhergestellt werden.

# 5 Sicherungsmodalitäten festlegen

## 5.1 Zeitpunkt de Backups bestimmen

Backups auf das NAS werden sofort durchgeführt. Auch die Backups in die Cloud werden sofort durchgeführt.

Die Synchronisation der beiden NAS wird jeden Tag um 24:00 durchgeführt. So sind die beiden NAS immer auf dem neusten Stand und auch die Daten.

## 5.2 Netzwerkauslastung

Beim Erstellen der Backups werden nur die aktuellen Änderungen geschrieben. So kann sichergestellt werden, dass die Daten sofort aktuell sind und die Netzwerkauslastung wird so klein wie möglich gehalten. Die Synchronisation der NAS wird beim Tageswechsel durchgeführt, eine Zeit in der das Netzwerk frei ist. Bei bedarf kann das Backup auch verschoben werden, um die Auslastung bei spontaner Planänderung möglichst klein zu halten.

## 5.3 Sicherungsbedarf

Aufgrund der hohen Erzeugung neuer Daten, ist auch der Sicherungsbedarf sehr gross. Somit müssen die Backups immer aktuell gehalten werden. Dies beruht darauf, dass viel mit den Daten gearbeitet wird.

## 5.4 Periodizität des Backups bestimmen

Aufgrund der grossen und vielen Änderungen der Daten muss immer alles aktuell gehalten werden. Somit wird bei jeder Änderung nach dem Arbeiten ein Backup erstellt. Die Synchronisation jedoch findet ein Mal am Tag statt.

## 5.5 Art und Anzahl der Backups bestimmen

Auf dem Core-NAS wird nur ein Backup der aktuellen Daten geschrieben. Auf dem Redundanz-NAS wird das Backup des Vortages mit aufbewahrt und das Aktuelle ebenfalls. Somit ist im Redundanz-NAS doppelt so viel Speicher verbaut wie im Core-NAS. Beide NAS sind mit einem Raid konfiguriert. Am sichersten ist dabei das Raid 10. Am platzsparendsten ist jedoch Raid 5. Raid 6 bietet die beste Möglichkeit dazwischen. Die Backups in der Cloud sind auf so vielen Geräten verfügbar, das heisst diese werden nicht noch ein Mal gesichert.

# 6 Speichermedien bestimmen

Als Speichermedien habe ich mich für zwei NAS, die Cloud und zwei externe Medien entschieden. Die NAS werden aus alter Hardware gebaut und sind somit leistungsfähiger als die meisten günstigen fertig NAS. Die Cloud ist extrem schnell und überall verfügbar. Die beiden Medien für die vertraulichen Daten sind klein und gut in einem kleinen Safe aufzubewahren.

## 6.1 NAS

Das NAS bietet sich an, um schnelle Backups und Restores zu machen. Sie sind meist leicht zu transportieren und können bei bedarf auch aufgerüstet werden. Meist sind sie auch günstiger als etliche CD’s zu kaufen. Die Daten können in der richtigen Umgebung überall hin transportiert werden.

## 6.2 Cloud

Das Backup in der Cloud bei GitHub ist extrem schnell und kann überall wo es Internet hat Restored werden. Bei GitHub können aber maximal 100MB grosse Dateien hochgeladen werden, da man ansonsten die Pro Version kaufen müsste. Das heisst für schnell verfügbare Dateien perfekt, da diese so gut wie immer unter 100MB sind.

## 6.3 USB-Stick und externe Festplatte

Diese sind sehr praktisch bei vertraulichen Daten. Sie können einfach verstaut werden und sind solange sie nicht angeschlossen sind auch nicht lesbar und hackbar.

## 6.4 3-2-1 Regel

- Sicherung auf dem Core-NAS
- Redundante Sicherung auf dem Redundanz-NAS
- Sicherung in der Cloud bei GitHub
- USB-Stick
- Externe Festplatte

Speichermedien bestimmen

## 6.5 2 Verschiedene Medien

- NAS
- Cloud
- USB-Stick
- Externe Festplatte

Sicherung ausser Haus

- Redundanz-NAS in Basel

## 6.6 Technische Aspekte

Das NAS muss schnell sein um die Daten im Notfall so schnell wie möglich wieder herstellen zu können. Damit das auch funktioniert wird das NAS mit ausreichend Festplatten ausgestattet. Die Anzahl der Festplatten kann aufgrund des verwendeten Gehäuses variieren.

### 6.6.1 Benötigter Speicherplatz

**Core-NAS**

6000GB + (500GB * 5Jahre) = 8500GB = 8.5TB

Für das Core-NAS müssen noch einige Festplatten organisiert werden, um diesen Speicherbedarf abzudecken.

**Redundanz-NAS**

12000GB + (100GB * 5Jahre) = 17000GB = 17TB

Das Redundanz-NAS deckt aktuell nicht annähernd den benötigten bedarf ab. Somit muss noch einiges investiert werden, um dies zu realisieren.

Speichermedien bestimmen

## 6.7 Betriebswirtschaftliche Aspekte

### Einmalige Installationskosten

- Arbeit von Yannick Morgenthaler 80.-/Std. x 6 Std. = 480.-

### Wiederkehrende Kosten

- Aufrüsten der Disks und Ersatz (es wird mit 6TB Disks gerechnet) 150CHF * 6 = 900.-

## 6.8 Ablauf eines Mehrstufigen Backups

Ich habe mich für ein mehrstufiges Backup mit folgenden Stufen entschieden:

- Stufe 1: Sicherung auf dem Core-NAS
- Stufe 2: Sicherung auf dem Redundanz-NAS
- Stufe 2: Sicherung aus der Cloud

Der Ablauf sieht wie folgt aus:

- Backups werden nach jeder Aktualisierung auf die ersten Medien geschrieben.
- Eine redundante Sicherung wird anschliessend alle 24h erstellt.

# 7 Sicherungssoftware bestimmen

## 7.1 Datensicherung

Die beiden NAS werden mit FreeNAS bzw TrueNAS umgesetzt. Diese werden anschliessend als Laufwerk im PC eingebunden. Somit fungiert das Core-NAS als persönliches Laufwerk. Die Synchronisierung der NAS basiert auf einem selbstgeschriebenen Skript, welches die Daten lediglich nach einem gewissen Muster kopiert und organisiert.

In der Cloud wird auf GitHub gesetzt, aufgrund der nicht vorhandenen Kosten und der hohen verfügbarkeit.

## 7.2 Sicherung des PC

Die ISO Dateien werden 1x im Monat manuell erstellt und auf das NAS geschoben.

## 7.3 Sicherung des Smartphones

Die Daten meines OnePlus 7 Pro können per NextCloud auf das NAS geschoben werden, dies kann automatisch gemacht werden oder manuell.

# 8 Aufbewahrung der Datenträger bestimmen

Bei der Lagerart und des Lagerorts muss auf einiges geachtet werden, damit die Datenträger nicht beschädigt werden. Da die beiden NAS rund um die Uhr in betrieb sind, ist bei der Aufbewahrung nur darauf zu achten, dass diese in einem geschützten Raum stehen. Sodass keine Feuchtigkeit oder anderes die elektronischen Bauteile beschädigen kann.

## 8.1 Datenschutzaspekte beachten

In einer Geschäftlichen Umgebung müssen gewisse Daten über mehrere Jahre aufbewahrt werden. Meist sind dies 10 Jahre. Im Privathaushalt muss nicht speziell darauf geachtet werden. Man sollte trotzdem darauf achten, dass nur der Besitzer der Daten darauf zugreiffen kann.

## 8.2 Zutrittskontrolle

Die mobilen Datenträger mit den vertraulichen Daten sind verschlüsselt und können nur mit Benutzername und Passwort entschlüsselt werden. Der Zugang zum Safe sollte ebenfalls kontrolliert werden.

## 8.3 Datenträger korrekt beschriften

Damit auf den ersten Blick erkennbar ist, auf welchem Datenträger sich was befindet, sollte man diese richtig beschriften, sodass alles zugeordnet werden kann. Im Betrieblichen Umfeld sollte ein Konzept für die richtige Beschriftung eingeführt werden. Im Privaten Umfeld reicht ein Stichwort.

## 8.4 Datenträger korrekt lagern

Die Harddisks im Safe sollten in der Anti Statischen Verpackung und in einem stossfesten Behälter aufbewahrt werden. Die USB-Sticks sollten regelmässig ersetzt werden.

# 9 Verantwortung für das Backup und Restore festlegen

## 9.1 Dateneigentümer

Yannick Morgenthaler. Ich bin für meine Daten verantwortlich.

## 9.2 Systemeigentümer

Yannick Morgenthaler. Ich bin für die Systeme verantwortlich.

## 9.3 Backupverantwortlicher

Yannick Morgenthaler. Ich bin für das Erstellen und Verwalten der Backups verantwortlich.

## 9.4 Backup-Systemverantwortlicher

Yannick Morgenthaler. Ich bin für die Backupsysteme verantwortlich.

## 9.5 Operator

Yannick Morgenthaler. Ich bin System Operator und Administrator. Mir unterliegen alle Systeme.

## 9.6 Qualitätsverantwortlicher

Yannick Morgenthaler. Ich bin für die Qualität der Backups verantwortlich.

# 10 Reflexion

Es steht schon lange eine solche Idee im Raum, doch ich bin nie dazu gekommen mir ein gutes Konzept dafür zu überlegen. So habe ich jetzt ein gut ausgearbeitetes Konzept, mit welchem ich das umsetzen kann und mir keine sorgen mehr machen muss um meine Daten.

## 10.1 Erkenntnisse

Mir wurde in den letzten Tagen immer mehr bewusst, wie wichtig Backups doch sind. Mir ist das schon ein Mal passiert, dass ich meine Daten verloren habe. Das wollte ich aber nicht noch einmal haben. Es geht aber vielen so und doch sind viele nicht wirklich begeistert von dieser Idee.

## 10.2 Was würde ich anderst machen

Viel zu viel was das allgemeine Arbeiten betrifft.

## 10.3 Schätzung der Note

Ich halte eine 5 für relativ realistisch.

# 11 Selbsständigkeitserklärung

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

Datensicherungskonzept_____

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 GIBM oder an einer anderen Ausbildungseinrichtung verwendet wurde.

## 11.1 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.

## 11.2 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 1*** | ***Autor 2*** | ***Autor 3*** |
|---|---|---|---|
| Name: | Morgenthaler____ | _____ | _____ |
| Vorname: | Yannick_____ | _____ | _____ |
| Datum: | 22.03.2022_____ | _____ | _____ |
| Unterschrift: | Y.Morgenthaler___ | _____ | _____ |

# 12 Quellen

- Lehrmittel
- Google
- Digitec