Software Verification Plan

**Projekt:**

Passwortmanager

**Autor:**

Software\_Verification\_Plan

**Datum:**

13.03.25

**Version:**

1.0

**Prüfer:**

Sascha Wanninger

**Freigabe durch autorisierte Person:**

Ekaterina Karavaeva

**Changelog:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Autor** | **Datum** | **Version** | **Änderung** |
| Hugo Hölzle | 13.03.25 | 1.0 | -------------- |
|  |  |  |  |
|  |  |  |  |

## 1. Einleitung

Dieser Software Verification Plan (SVP) beschreibt die Methoden, Strategien und Kriterien, die zur Verifizierung des Passwort-Managers in Python verwendet werden. Ziel ist es, sicherzustellen, dass die Software die funktionalen und nicht-funktionalen Anforderungen erfüllt.

## 2. Verifikationsstrategie

Die Verifikation des Passwort-Managers erfolgt in mehreren Phasen, einschließlich statischer Analyse, dynamischer Tests und Sicherheitsprüfungen.

## 3. Testmethoden und Werkzeuge

- Unittests: Nutzung von `unittest` für modulare Tests  
- Code Coverage:\*Prüfung der Testabdeckung (Mindestwert: 75%)  
- Statische Analyse:\*Verwendung von pylint zur Code-Qualitätsprüfung  
- Typprüfung: Nutzung von mypy zur statischen Typprüfung  
- Sicherheitsanalyse:bÜberprüfung der Verschlüsselungsimplementierung und API-Anbindung

## 4. Verifikationskriterien

Die Software wird anhand der folgenden Kriterien überprüft:

- Funktionale Anforderungen: Korrekte Implementierung aller definierten Funktionen  
- Sicherheit: Schutz der gespeicherten Daten durch starke Verschlüsselung  
- Zuverlässigkeit: Fehlerfreie Ausführung ohne Abstürze  
- \*\*Benutzerfreundlichkeit: Intuitive Menüführung und klare Anweisungen  
- \*\*Performance: Angemessene Laufzeit für alle Operationen

## 5. Testfälle und Szenarien

- Passwortspeicherung: Testen der sicheren Speicherung und Verschlüsselung  
- Passwortgenerierung: Überprüfung der generierten Passwörter nach Sicherheitsrichtlinien  
- Passwortabruf: Sicherstellen, dass gespeicherte Passwörter korrekt abgerufen werden  
- Passwortbearbeitung: Verifizierung von Änderungs- und Löschfunktionen  
- Master-Passwort: Prüfung der sicheren Speicherung und Authentifizierung  
- Nutzermanagement: Testen der Multi-Account-Funktionalität  
- Import/Export: Sicherstellen der korrekten Datenübertragung zwischen CSV und JSON

## 6. Fehlerverfolgung und Berichterstattung

Gefundene Fehler werden über ein Issue-Tracking-System dokumentiert. Jeder Fehler wird nach Schweregrad kategorisiert und priorisiert.

## 7. Abschluss und Freigabe

Die Software wird als verifiziert betrachtet, wenn alle definierten Tests bestanden wurden und keine kritischen Fehler vorliegen.