|  |  |  |  |
| --- | --- | --- | --- |
| **Daten** | **Nutzer** | **Rechte** | **Schutzklasse** |
| Grundrissplan | Vermesser | Lesen und schreiben | 3 |
|  | Planung | leserecht |  |
| Auftragsdaten | Kunde | leserecht | 3 |
|  | Bearbeiter | Lesen und schreiben |  |
| Lager | Lagerist | Lesen und schreiben | 2 |
|  | Einkauf | leserecht |  |
|  | Planung | leserecht |  |
| Persönliche Kundendaten | Planung | leserecht | 3 |
|  | Bearbeiter | Lesen und schreiben |  |

Schritt 6

Schritt 7

**Authentizität:**

Zuweisung von Zugriffsrechten bzw. Schreib-/Leserecht von Datenbanken  
Nicht Jeder Anwender ist berechtigt die Daten zu sehen, oder Änderungen an Daten vorzunehmen.  
Hierfür werden Accounts für die jeweiligen Nutzer angelegt, welche ein Passwort von mindestens 8 Zeichen (Zahlen, Groß- und Kleinschreibung und Zeichen) haben.  
Passwörter sind nur für die Person oder Personengruppe bestimmt. Jeder Mitarbeiter bekommt einen eigenen Login, welcher nur vom Admin ausgelesen werden kann.

So wird gewährleistet, dass in Hinsicht der Autorität nur die berechtigten Nutzer auf die Daten zugreifen können und gegebenen falls wird diese Änderung auch protokolliert.

**Verfügbarkeit:**

Um die Verfügbarkeit von Daten zu gewähren wird ein regelmäßiges Backup der Dateien aus dem Datenserver, auf einen Cloudserver und ein externes Laufwerk durchgeführt. Falls es zu einem Ausfall des ersten Datenträgers kommt, kann so unter minimalem Verlust der Daten der zweite Datenträge eingesetzt werden bzw. die Daten aus der Cloud gezogen werden, sobald die Hardware erneuert wurde.

Zudem sollten immer Ersatzhardwareteile vorhanden sein, falls ein Bauteil ausfällt.

**Für Cloud und Home Office**  
Die Clients sollen über einen verschlüsselten VPN Tunnel und eine Firewall eine Verbindung zum Ethernet herstellen können und sich mittels Login auf ihren Accounts einloggen können.  
So ist es möglich, das die Mitarbeiter von überall aus arbeiten können.  
Voraussetzung ist ein sicheres Arbeitsumfeld um die Vertraulichkeit der Daten zu garantieren.  
  
**Vertraulichkeit**

Zugriff unberechtigter dritter auf Daten muss unterbunden werden und ein Arbeitsplatz vorhanden sein welcher verhindert das dritte über die Schulter schauen können und USB Sticks müssen grundsätzlich verschlüsselt sein.

E-Mails müssen auch eine 1 zu 1 Verschlüsslung haben und gegeben Falls eine Authentifizierung via Passwort besitzen.