

Passwortschutzkarte für den sicheren Umgang mit Zugangsdaten

Diese Karte dient der sicheren Dokumentation und Verwaltung von Passwörtern und Zugangsdaten für den kirchlichen Gebrauch. Bitte bewahren Sie dieses Dokument sicher und getrennt von digitalen Geräten auf.

1. Allgemeine Hinweise zur Passwortsicherheit

- Verwenden Sie für jedes System ein eigenes, starkes Passwort.
- Nutzen Sie möglichst eine Zwei-Faktor-Authentifizierung (z. B. per App oder SMS).
- Ändern Sie Passwörter regelmäßig (z. B. alle 6–12 Monate).
- Verwenden Sie keine einfachen oder bekannten Begriffe (wie Namen, Geburtsdaten, „123456“).
- Geben Sie Passwörter **niemals** weiter – auch nicht an Kolleg:innen oder IT-Dienste.
- Schreiben Sie Passwörter **nicht sichtbar** auf Zettel oder Bildschirme.

2. Passwortdokumentation (Beispiel-Tabelle)

System/Dienst	Benutzername	Passwort (nicht öffentlich notieren!)	Letzte Änderung
E-Mail (Outlook/Office)	max.mustermann	●●●●●●●●	01.01.2025
Cloud-Speicher	gemeinde-intern	●●●●●●●●	15.03.2025
Webseite (CMS)	admin.gemeinde	●●●●●●●●	05.02.2025
Kirchenverwaltungsportal	pastor.musterhausen	●●●●●●●●	20.04.2025
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

 **Tipp:** Nutze zur Passwortspeicherung einen sicheren Passwortmanager. Auf dieser Karte kannst du dann nur den Verwendungszweck und Benutzername notieren – ohne das eigentliche Passwort.

3. Notfallhinweis

Diese Passwortkarte darf **ausschließlich autorisiertem Personal** zugänglich gemacht werden.

Bei Verlust oder Verdacht auf unbefugte Nutzung bitte **sofort den IT-Beauftragten** oder den Datenschutzverantwortlichen der Kirchengemeinde kontaktieren.