Informatik	**Gemeinde:**	Muster-Kirchgemeinde
	Rechnungsjahr:	Muster-Rechnungsjahr
	Prüfungsdatum:	Muster-Prüfungsdatum
	Visum:	

1	**Prüfungsziel**	
	Der effiziente Einsatz von Informatikmitteln ist sichergestellt. Es ist eine zweckmässige Datensicherung vorhanden. Es bestehen keine wesentlichen Informatikrisiken ohne zweckmässige Kontrollmassnahmen. → Die Prüfungstätigkeit mittels dieser Checkliste stellt nur eine Grobbeurteilung dar.	
2	**Prüfungsgrundlagen**	
	Rechtsgrundlagen, z.B. - Informatikgesetz, SRL Nr. 026	- Inventare Hard- und Software - Wartungs- und Software-Verträge - Berichte von Informatikprüfungen von Fachpersonen - Zugriffskonzept - Beschreibung Arbeitsabläufe

3	**Prüfungshandlungen**	**Prüfungsergebnis**
3.1	Wurde der Bereich Informatik durch externe Fachpersonen detailliert geprüft (Informatikrevision)? → Bericht einsehen, Stand der Umsetzung von wesentlichen Bemerkungen prüfen und Ergebnisse in die Prüfungshandlungen einbeziehen.	☐ ja ☐ nein Beilagen:
3.2	Sind die Verantwortlichkeiten für den Informatikeinsatz klar geregelt (inkl. Stellvertretungen auf allen Stufen)? → Beurteilung der Regelungen gemeindeintern sowie gemeinsam mit externen Fachpersonen / Firmen. Abhängigkeiten von einzelnen Personen möglichst vermeiden. Ausreichende Funktionentrennung (z.B. zwischen Informatik und Rechnungswesen) sicherstellen.	☐ ja ☐ nein Beilagen:
3.3	Falls externe IT-Unterstützung beigezogen wird: Wer sind die Partner und wie ist die Zusammenarbeit geregelt? → Adressverzeichnisse sowie (Dienstleistungs-)Vereinbarungen und (Wartungs-) Verträge etc. einsehen. Prüfen, ob Vertraulichkeit, Zugang zu den Systemen und der Überwachung geregelt sind.	☐ ja ☐ nein Beilagen:
3.4	Besteht ein Verzeichnis oder ein Inventar der eingesetzten Hardware und Software? → Verzeichnis / Inventar einsehen, mit Angaben in der Anlagebuchhaltung / Bestandesrechnung vergleichen	☐ ja ☐ nein Beilagen:
3.5	Besteht eine Übersicht der eingesetzten Software-Anwendungen und deren Schnittstellen untereinander? → Übersicht einsehen (falls vorhanden) respektive gemeinsam mit der für die IT verantwortlichen Person erstellen, Schnittstellen (Art sowie Kontrolle und Nachvollzug der Schnittstellen-Verarbeitung) aufnehmen.	☐ ja ☐ nein Beilagen:

3.6	Können Veränderungen an den Stammdaten (zum Beispiel Debitoren) sowie die zentralen Tabellen und Parameter der Applikationen nur durch berechtigte Personen vorgenommen werden? → Prüfen, wer die Stammdaten pflegt und ob Änderungen nachgewiesen werden (z.B. mittels Systemprotokolle, History oder Belegen).	☐ ja ☐ nein Beilagen:
3.7	Sind die Vergabe und die periodische Überprüfung der Zugriffsrechte sinnvoll geregelt? → Eingeschränkte Zugriffe, Art der Zugriffsberechtigung (abfragen / ändern), Aktualisierung (z.B. bei Eintritten und Austritten sowie internem Funktionswechsel von Anwendern), Zugriffe auf den Gemeindeserver "von aussen" via Internet, Bildschirm-Logout bei längerer Inaktivität etc. Vgl. Zugriffskonzept, falls vorhanden.	☐ ja ☐ nein Beilagen:
3.8	Ist ein sinnvolles Passwortsystem vorhanden? → Periodizität der Aktualisierung von Passwörtern prüfen. Sicherstellen, dass Zugriff auf Daten nur mittels Passwort vorgenommen werden kann.	☐ ja ☐ nein Beilagen:
3.9	Existieren klare interne Regelungen, welche Daten nach "aussen" publiziert werden dürfen (Internet)?	☐ ja ☐ nein Beilagen:
3.10	Ist eine zweckmässige Datensicherung (Schutz vor Datenverlust) sichergestellt? → Vgl. Datensicherungskonzept, falls vorhanden. Einhaltung prüfen.	☐ ja ☐ nein Beilagen:
3.11	Werden die gesicherten Daten zweckmässig aufbewahrt? → Aufbewahrung intern in einem Datenträger-Safe. Aufbewahrung periodisch an einem externen Ort. Prüfen, ob Lesbarkeit der gesicherten Daten sichergestellt ist. Prüfen, ob Datensicherungen vor unbefugtem Zugriff geschützt sind.	☐ ja ☐ nein Beilagen:
3.12	Ist ein zweckmässiger Virenschutz sichergestellt? → Prüfen, ob Aktualisierung der Virenschutz-Software gewährleistet ist. Prüfen, ob Virenschutz auch bei Downloads vom Internet sichergestellt ist.	☐ ja ☐ nein Beilagen:
3.13	Besteht ein Notfallkonzept für Katastrophenfälle wie z.B. Totalausfall der IT-Systeme oder Virenbefall? → Prüfen, ob verantwortliche Person bestimmt, die Mitarbeitenden informiert und entsprechende Massnahmen vorgesehen sind.	☐ ja ☐ nein Beilagen:
3.14	Ist ein zweckmässiger Schutz des Netzwerkes mit einer Firewall sichergestellt? → Prüfen, wer "von aussen" (Internet, Modem etc.) in welcher Form und auf welche Daten zugreifen kann.	☐ ja ☐ nein Beilagen:
3.15	Sind die zentralen IT-Infrastrukturen ausreichend geschützt? → Zutrittsbeschränkungen zum Serverraum, Wasser- und Feuerschutz, unterbrechungsfreie Strom-Versorgung etc.	☐ ja ☐ nein Beilagen:
3.16	Gibt es wesentliche Probleme mit der eingesetzten Soft- und Hardware? → Hinterfragen, ob grössere Probleme aufgezeichnet und analysiert (was lernt man aus Vorfällen?) werden.	☐ ja ☐ nein Beilagen:

3.17	Genügen die vorhandenen Ressourcen in quantitativer und qualitativer Hinsicht für eine wirksame Unterstützung der Anwenderinnen und Anwender sowie die Pflege der installierten Hard- und Software?	☐ ja ☐ nein Beilagen:
3.18	Bei Vorhandensein einer zentralen Datenbank (z.B. Rechenzentrum): Wurde bei der Erstellung der Datenbank durch die zuständige Behörde eine genehmigte Leistungsvereinbarung abgeschlossen? → Vereinbarung einsehen. Vgl. Informatikgesetz.	☐ ja ☐ nein Beilagen:
3.19	Ist eine Regelung / Weisung vorhanden zum Umgang mit E-Mail, Internet und Passwörtern, Installation von eigener Software etc.? → Prüfen, ob diese den Mitarbeitenden bekannt sind (z.B. Schulung bei Eintritt).	☐ ja ☐ nein Beilagen:
3.20	Besteht eine mittel- und langfristige IT-Strategie und –Planung?	☐ ja ☐ nein Beilagen:
3.21	Erfolgen Beschaffungen im IT-Bereich in Übereinstimmung mit der mittel- und langfristigen IT-Strategie und –Planung sowie unter Einhaltung der Finanzkompetenzen?	☐ ja ☐ nein Beilagen:
3.22	Sind die Verantwortlichkeiten und Verfahren bei Programmanpassungen oder Releasewechseln (neue Version Software) klar geregelt? → Prüfen, ob ein Testkonzept vorhanden ist (z.B. Testumgebung, Freigabe der Änderungen durch die verantwortlichen Benützer, Testdokumentation).	☐ ja ☐ nein Beilagen:
	Risikobeurteilung	
3.23	Zusätzliche Prüfungshandlungen aus Risikobeurteilung:	Ergebnis: Beilagen:
4	**Feststellungen**	
5	**Fazit**	
5.1	Abschliessende Beurteilung	
5.2	Feststellungen für die Berichterstattung ☐ ja ☐ nein	