**Beispiel für ein Dokument zur Planung von Gruppenrichtlinien unter Windows**

**Dokumenttitel:** Richtlinie zur Planung, Implementierung und Verwaltung von Gruppenrichtlinien (GPO) in der Windows-Domäne

**Dokumenten-ID:** 2 **Version:** 1.0 **Erstellungsdatum:** 2025-05-22 **Letzte Überarbeitung:** 2025-05-22 **Autor:** XXX **Genehmigt durch:** XXX

**1. Einleitung**

Dieses Dokument beschreibt die Richtlinien und Prozesse für die Planung, Implementierung und Verwaltung von Gruppenrichtlinien (Group Policy Objects - GPOs) innerhalb unserer Windows Active Directory-Umgebung. Ziel ist es, eine konsistente, sichere und effiziente Konfiguration unserer IT-Systeme zu gewährleisten, Compliance-Anforderungen zu erfüllen und die administrative Last zu reduzieren.

**2. Geltungsbereich**

Diese Richtlinie gilt für alle Windows-basierten Server, Clients und Benutzerkonten, die in unserer Active Directory-Domäne verwaltet werden. Dies umfasst alle Phasen des GPO-Lebenszyklus, von der Planung bis zur Außerbetriebnahme.

**3. Ziele der GPO-Verwaltung**

* **Sicherheit:** Durchsetzung von Sicherheitsvorgaben (z.B. Passwortrichtlinien, Firewall-Regeln, Software-Einschränkungen).
* **Compliance:** Erfüllung interner und externer Compliance-Anforderungen (z.B. DSGVO, BSI-Grundschutz).
* **Effizienz:** Automatisierung der Systemkonfiguration und Reduzierung manueller Eingriffe.
* **Standardisierung:** Sicherstellung einer einheitlichen Systemkonfiguration über alle betroffenen Systeme hinweg.
* **Transparenz:** Klare Dokumentation aller GPOs und ihrer Auswirkungen.

**4. Rollen und Verantwortlichkeiten**

|  |  |  |
| --- | --- | --- |
| **Rolle** | **Verantwortlichkeiten** | **Owner\_ID** |
| **Global ICT** | Gesamtverantwortung für die GPO-Strategie, Architektur und Haupt-Implementierung. Erstellung und Pflege der Haupt-GPOs. | 31 |
| **IT-Infrastruktur** | Implementierung und Pflege von GPOs, Fehlerbehebung, Überwachung der GPO-Anwendung. | 31 |
| **IT-Sicherheit** | Definition und Überprüfung von Sicherheitsanforderungen für GPOs. | 33 |
| **Fachabteilungen** | Definition von spezifischen Anwendungsanforderungen, die über GPOs umgesetzt werden sollen. | N/A |
| **CTO** | Genehmigung der GPO-Richtlinie und wichtiger Änderungen. | 32 |
| **Auditor** | Überprüfung der Einhaltung dieser Richtlinie. | 28 |

In Google Sheets exportieren

**5. Planungsprozess für neue GPOs/Änderungen an bestehenden GPOs**

Jede neue GPO oder wesentliche Änderung an einer bestehenden GPO muss einem definierten Planungsprozess folgen:

1. **Anforderungsanalyse:**
   * Klare Definition der Anforderung (Was soll erreicht werden? Welches Problem wird gelöst?).
   * Identifikation der betroffenen Benutzer/Systeme.
   * Bewertung der Sicherheitsauswirkungen.
   * Einbeziehung relevanter Stakeholder (Fachabteilungen, IT-Sicherheit).
2. **Konzeption und Design:**
   * Entwurf der GPO-Einstellungen.
   * Überprüfung auf mögliche Konflikte mit bestehenden GPOs.
   * Definition der Verknüpfungsstrategie (OU-Link, Domänen-Link).
   * Festlegung von Filtern (Sicherheitsfilterung, WMI-Filter).
   * Namenskonventionen: GPO-<Funktion>-<Ziel> (z.B. GPO-Passwortrichtlinie-Domäne, GPO-SoftwareInstallation-Buchhaltung).
   * Dokumentation des GPO-Zwecks und der Einstellungen.
3. **Testphase:**
   * Implementierung der GPO in einer Testumgebung (separate OU für Tests).
   * Gründliche Tests der Funktionalität und potenzieller Nebeneffekte.
   * Einbeziehung von Testbenutzern aus den betroffenen Bereichen.
4. **Implementierung und Rollout:**
   * Geplanter Rollout in der Produktionsumgebung (ggf. schrittweise).
   * Überwachung der Anwendung der GPO und der Systemreaktionen.
   * Kommunikation an betroffene Benutzer, falls relevant.
5. **Überprüfung und Wartung:**
   * Regelmäßige Überprüfung der GPO-Wirksamkeit (mindestens jährlich).
   * Anpassung der GPOs an neue Anforderungen oder Sicherheitsrisiken.
   * Entfernung veralteter oder nicht mehr benötigter GPOs.

**6. Technische Aspekte und Best Practices**

* **Verknüpfungsstrategie:** GPOs sollten so nah wie möglich am Zielobjekt verknüpft werden (OU-Link vor Domänen-Link), um die Verarbeitung zu optimieren und Konflikte zu minimieren.
* **Vererbung und Blockierung:** Die Blockierung der Vererbung sollte nur in begründeten Ausnahmefällen und mit Genehmigung des Global ICT Teams erfolgen.
* **WMI-Filter:** Sparsamer Einsatz von WMI-Filtern aufgrund der Performance-Auswirkungen. Klare Dokumentation jedes Filters.
* **Sicherheitsfilterung:** Präzise Definition der Sicherheitsfilterung, um sicherzustellen, dass GPOs nur auf die vorgesehenen Gruppen angewendet werden.
* **Notfallprozesse:** Definition von Prozessen zur schnellen Deaktivierung oder Wiederherstellung von GPOs im Falle von Problemen. Nutzung von GPO-Backup-Funktionen.
* **Versionierung und Backup:** Regelmäßige Sicherung aller GPOs und Versionierung von Änderungen.
* **Dokumentation:** Jede GPO muss dokumentiert werden, einschließlich:
  + Zweck der GPO
  + Betroffene Objekte (Benutzer, Computer, OUs)
  + Wesentliche Einstellungen
  + Verknüpfungsort
  + Sicherheitsfilter
  + Datum der letzten Änderung und verantwortlicher Mitarbeiter
  + Gültigkeitsdauer (falls befristet)

**7. Überwachung und Auditierung**

* Regelmäßige Überprüfung der GPO-Anwendung und des GPO-Ergebnissatzes (Resultant Set of Policy - RSoP) auf Stichproben.
* Protokollierung von Änderungen an GPOs im Active Directory.
* Regelmäßige Audits der GPO-Struktur und -Einstellungen durch das IT-Sicherheitsteam oder externe Auditoren.

**8. Richtlinienkonformität und Abweichungen**

Abweichungen von dieser Richtlinie sind nur in begründeten Ausnahmefällen und mit schriftlicher Genehmigung des CTOs (ID 32) zulässig. Alle Abweichungen müssen dokumentiert und regelmäßig überprüft werden.

**9. Dokumentenüberprüfung**

Dieses Dokument wird jährlich durch das Global ICT Team überprüft und bei Bedarf aktualisiert.