Google Admin: Grundlegende Einrichtung

Diese Checkliste soll IT-Administratoren bei der Einrichtung von Google Workspace gemäß den Best Practices unterstützen.

Die Befolgung dieser Checkliste hilft Ihnen, Ihre Organisationsstruktur zu optimieren, sie einfach, übersichtlich und sicher zu halten und den Datenschutz sicherzustellen.

 # 0. Super-Administration

☐ Weisen Sie die Super-Admin-Rolle 1–2 Schlüsselpersonen für das oberste Management zu.
☐ Schützen Sie Super-Admin-Rollen mit zusätzlichen Authentifizierungsmechanismen (z. B. Schlüssel/Zertifikate).
☐ Verwenden Sie weniger privilegierte Admin- und Nicht-Admin-Konten für reguläre Aktivitäten.
☐ Überprüfen und auditieren Sie regelmäßig Admin-Rollen.

 # 1. Organisationsstruktur

☐ Erstellen Sie eine Organisationsstruktur in der Google Admin-Konsole.
☐ Definieren Sie Organisationseinheiten (OUs) für Teams, Abteilungen oder Geschäftsbereiche.
☐ Weisen Sie Benutzer den entsprechenden Organisationseinheiten zu.
☐ Wenden Sie spezifische Richtlinien auf jede Organisationseinheit an.

 # 2. Benutzerkonten, Rollen und Berechtigungen

☐ Erstellen Sie Benutzerkonten für alle Mitarbeiter.
☐ Erstellen Sie Benutzerrollen und richten Sie Sicherheitsberechtigungen basierend auf den Jobanforderungen ein.
☐ Weisen Sie Benutzer entsprechend Ihrer Organisationsstruktur ihren Rollen zu.
☐ Begrenzen Sie Admin-Berechtigungen auf eine minimale Anzahl von Benutzern.
☐ Überprüfen und aktualisieren Sie regelmäßig Benutzerrollen und Berechtigungen.

 # 3. Allgemeine Sicherheitseinstellungen

☐ Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für alle Konten.
☐ Erzwingen Sie starke Passwortrichtlinien (z. B. Länge, Komplexität und Ablauf).
☐ Richten Sie Warnmeldungen für verdächtige Kontoaktivitäten ein.

☐ Konfigurieren Sie Sitzungs-Timeout-Richtlinien, um Benutzer nach Inaktivität automatisch abzumelden.

 # 4. Allgemeines Gerätemanagement

☐ Registrieren Sie alle Unternehmensgeräte in der Google Workspace-Geräteverwaltung.
☐ Richten Sie Richtlinien für verlorene oder gestohlene Geräte ein (z. B. Fernlöschung).
☐ Erfordern Sie Geräteeinstellungen für Verschlüsselung aller Endpunkte, die auf Unternehmensdaten zugreifen.
☐ Stellen Sie sicher, dass Unternehmensgeräte über aktuelle Antivirus- und Firewall-Software verfügen.

 # 5. Datenzugriffskontrolle

☐ Konfigurieren Sie Zugriffsbeschränkungen für Google Drive, Docs, Sheets und andere Dienste.
☐ Verwenden Sie geteilte Laufwerke für die Teamzusammenarbeit mit eingeschränktem Zugriff.
☐ Legen Sie Ablaufdaten für das Teilen von Dateien mit externen Parteien fest.
☐ Auditieren Sie regelmäßig die Freigabeeinstellungen für sensible Daten.

 # 6. E-Mail- und Kommunikationssicherheit

☐ Aktivieren Sie E-Mail-Verschlüsselung (TLS) für sichere Kommunikation.
☐ Richten Sie E-Mail-Filter für Phishing- und Spam-Erkennung ein.
☐ Konfigurieren Sie ausgehende E-Mail-Beschränkungen für sensible Daten.
☐ Verwenden Sie Google Vault, um E-Mails für Compliance- Anforderungen zu archivieren.

 # 7. Überwachung und Berichterstellung

☐ Richten Sie die Protokollierung von Admin-Aktivitäten in der Google Admin-Konsole ein.
☐ Überprüfen Sie regelmäßig Sicherheitsberichte und Protokolle auf ungewöhnliche Aktivitäten.
☐ Verwenden Sie das Sicherheits-Dashboard, um potenzielle Risiken im Überblick zu behalten.
☐ Konfigurieren Sie automatische Warnmeldungen für Sicherheitsvorfälle.

 # 8. Schulung und Bewusstsein

☐ Bieten Sie Schulungen für Mitarbeiter zu Best Practices in Google Workspace an.
☐ Schulen Sie Benutzer zu Phishing- und Cybersecurity-Bewusstsein.
☐ Erstellen Sie ein Richtliniendokument für die akzeptable Nutzung von Google Workspace-Tools.
☐ Ermutigen Sie zu regelmäßigem Feedback zu Benutzerfreundlichkeit und möglichen Verbesserungen.

Brauchen Sie beim nächsten Schritt Hilfe?

Wenn Sie zu einem dieser Schritte eine Frage haben oder Hilfe beim Einrichten einer fortgeschritteneren oder maßgeschneiderten Lösung benötigen, sind wir für Sie da!

Senden Sie uns einfach eine E-Mail an contact@403bits.com.

Bei einfacheren Fragen geben wir Ihnen gerne Ratschläge oder weisen Sie in die richtige Richtung – kostenlos!

Und wenn Sie vor einer komplexeren Herausforderung stehen oder Zeit sparen möchten, können unsere Experten übernehmen und eine umfassende Einrichtung bereitstellen, die perfekt zu Ihren Anforderungen passt.

Wir sind hier, um Ihnen beim Aufbau von Sicherheit und Effizienz zu helfen, damit Sie sich auf das Wachstum Ihres Unternehmens konzentrieren können!

Wenn Ihnen diese Checkliste gefallen ist oder Sie Verbesserungsvorschläge haben, lassen Sie es uns unter contact@403bits.com wissen.