Step-by-Step Guide

mesaforte Firefighter

Temporärere Zugriffe auf kritische Systeme müssen sicher und überprüfbar sein. mesaforte.Firefighter bietet eine einfache Lösung: kontrollierter, zeitlich begrenzter Zugriff für Notfälle, Projekte oder Urlaubsvertretung.

Schritt 1
Identifizieren Sie den Bedarf an temporären Zugriffe

- Bestimmen Sie, warum erhöhte Rechte benötigt werden (z.B. Notfall, Projekt, Urlaubsvertretung).
- Stellen Sie sicher, dass der Zugang zeitlich begrenzt und klar begründet ist.

- ***Essentiell:*** *Verwenden Sie niemals permanente high-level Zugangsrechte für kurzfristige Zweckee. Verwenden Sie stattdessen Firefighter.*

Schritt 2
Erstellen eines Rollenkatalogs

- Bestimmen Sie, welche zusätzlichen SAP-Rollen zur Erfüllung einer kritischen Aufgabe benötigt werden. Beachten Sie bitte, dass der Nutzer diese temporären Rechte zusätzlich zu seinen dauerhaften Rechten erhalten wird.
- Erstellen Sie eine temporäre Rolle (z.B. Code Red, Code Blue, etc.).
- Definieren Sie Systemumfang, verfügbare Funktionen und Dauer.

- ***Essentiell:*** *Benennen Sie die Rolle entsprechend dem Zugriffszweck (z. B. „Code White - HR Vacation Backup“).*

Schritt 3
Zuweisung der Rolle an den Benutzer

- Anwender die richtige Firefighter Rolle zugeweisen.
- Legen Sie ein Zeitlimit fest und bestimmen Sie den/die zuständigen Verantwortliche(n) für die Genehmigung.

- ***Essentiell:*** *Vermeiden Sie uneingeschränkte Zugrifef. Begrenzen Sie Umfang und Zeit.*

Schritt 4
Anfrage– und Genehmigungsworkflow

- Benutzer stellt Antrag
- Verantwortlicher erhält Meldung und genehmigt
- Nach Genehmigung wird der Zugang automatisch für den festgelegten Zeitraum aktiviert.

- ***Essentiell:*** *Transparente und überprüfbare Antrags-/Genehmigungskette gewährleistet die Einhaltung der Vorschriften.*

Schritt 5
Ausführen der Aufgaben

- Der Benutzer führt die ihm zugewiesenen Aufgaben in SAP mit erweiterten Rechten aus.
- Alle Aktivitäten werden automatisch protokolliert.

- ***Essentiell:*** *Die Benutzer müssen ihre Aktivitäten nicht manuell dokumentieren - alles wird automatisch erledigt.*

Schritt 6
Audit und Forensik

- Nach Ablauf der Zugriffszeit prüfen Auditoren oder Administratoren die Protokolle
- Logs können nach Benutzer, Tabellen, Transaktionen und Zeit gefiltert werden.
- Die Anzeige von Vorher-/Nachher-Datenwerten sorgt für volle Transparenz.
- Der Sign-off-Prozess hebt besonders kritische Aktionen für den Genehmiger der Protokolle hervor.

- ***Essentiell:*** *Audit-Funktionen reduzieren den Bedarf an manuellen Kontrollen.*

VORTEILE IM ÜBERBLICK

1. **Weniger Risiko** - Kein Bedarf an statischen High-Level-Rollen; temporärer Zugriff wird immer überwacht.
2. **Weniger Kontrollaufwand** – Automatisierte Genehmigungen und revisionssichere Protokolle vereinfachen die Einhaltung von Vorschriften.
3. **Höhere Flexibilität während des Urlaubs** – Einfaches Delegieren von Verantwortlichkeiten während der Abwesenheit wichtiger Mitarbeiter.
4. **Geld sparen** – Reduziert den IT- und Audit-Aufwand, vermeidet kostspielige Zugriffsverletzungen und unnötige Lizenzkosten
5. **Den guten Ruf aufrechterhalten** – Verhindert nicht-konformes Verhalten; gewährleistet Rückverfolgbarkeit.
6. **Sorgenfrei in den Urlaub fahren** – Kritische Zugriffe können sicher und ohne Stress gehandhabt werden.