Headless CMS Güvenlik, Backup & Disaster Recovery Planlama Şablonu — Yazılım / Security & DR (v1.0)

Asset Amaç: Bu audit sheet; headless CMS mimarinizin güvenlik yüzeylerini (RBAC, 2FA/IP kısıtlamaları, token ve secret anahtar yönetimi) ve iş sürekliliği katmanını (yedekleme, geri yükleme ve felaket kurtarma senaryoları) tek bir merkezi yapıda değerlendirip skorlamanızı sağlar. SaaS veya self-hosted sorumluluk matrisiyle "kim, hangi kriz anında neyi yapacak?" sorusunu netleştirerek kurumsal markalarda ve ajans süreçlerinde düzenli bir DR tatbikat döngüsü kurmayı amaçlar.

Kim Kullanır?: Teknik Liderler (Tech Lead), Siber Güvenlik Sorumluları, Ajans Teknik Proje Yöneticileri (PM) ve Altyapı/Operasyon Liderleri.

Nasıl Kullanılır?

1. Headless CMS altyapınızın mevcut güvenlik ve yedekleme yapılandırmasını 5 ana başlıkta 0-5 arası puanlayarak mevcut durum skorlamasını yapın.
2. Çıkan Kırmızı, Sarı veya Yeşil risk alanlarına göre eksik gedikleri tespit edin ve ilk 10 acil operasyonel aksiyon planını netleştirin.
3. İlk 14 günlük sprint içinde minimum güvenlik katmanını, çoklu yedekleme rutinini ve iletişim runbook'unu devreye alarak canlı bir veri geri yükleme (restore) testi gerçekleştirin.

TEMPLATE — Headless CMS Güvenlik, Backup & Disaster Recovery Planlama Matrisi

A) Güvenlik & İş Sürekliliği Olgunluk Skoru (0–5)

Sistem altyapısının siber tehditlere ve veri kayıplarına karşı dayanıklılığını ölçen teknik metrikler:

- **RBAC / 2FA / IP Olgunluğu (0–5):** ___ *(0: Herkes admin yetkili, iki aşamalı doğrulama yok - 5: Rol bazlı yetkilendirme aktif, 2FA zorunlu, panel erişimi IP korumalı)*
- **Token / Secret Yönetimi (0–5):** ___ *(0: API token'lar kod içinde sert yazılmış, rotasyon yok - 5: Environment variable seviyesinde gizli, düzenli otomatik rotasyon yapılıyor)*
- **Backup (Yedekleme) Kapsamı (0–5):** ___ *(0: Yedek alınmıyor - 5: Ham içerik, şema mimarisi, medya kütüphanesi ve sistem ayarları asenkron ve yedekli saklanıyor)*
- **Restore (Geri Yükleme) Test Olgunluğu (0–5):** ___ *(0: Yedeklerin çalışıp çalışmadığı hiç denenmedi - 5: Her ay otomatik veya manuel canlı restore tatbikatları yapılıyor)*
- **DR Runbook + İletişim Planı (0–5):** ___ *(0: Kriz anında kiminle konuşulacağı belirsiz - 5: Adım adım felaket senaryosu klavuzu hazır, paydaş iletişim matrisi net)*

$$\text{Toplam Altyapı Risk Skoru} = \text{Tüm Olgunluk Puanlarının Toplamı} \quad (\text{Maksimum: } 25)$$

B) Stratejik Risk ve Karar Yorum Alanları

- 🔴 **KIRMIZI (Kritik Seviye / Skor: 0–9):** Altyapı felaketlere açık, veri kaybı riski çok yüksek ve siber güvenlik açıkları barındıran acil müdahale bölgesi:
  _____
- 🟡 **SARI (Geliştirilmesi Gereken / Skor: 10–18):** Temel yedekler alınıyor ancak test edilmiyor; token yönetimi ve rol yetkilerinde boşluklar bulunan planlı iyileştirme hattı:
  _____
- 🟢 **YEŞİL (Tam Güvenli ve Sürdürülebilir / Skor: 19–25):** Veri yedekliliği kusursuz çalışan, yetkilendirmeleri sıkı, kriz senaryoları tatbikatlarla doğrulanmış güvenli liman:
  _____

C) İlk 10 Operasyonel Aksiyon Listesi (Sistem Sıkılaştırma Öncelikleri)

1. **Aksiyon 01 (Güvenlik / Altyapı):**
   _____
   _____
2. **Aksiyon 02 (Güvenlik / Altyapı):**
   _____
   _____
3. **Aksiyon 03 (Güvenlik / Altyapı):**
   _____
   _____
4. **Aksiyon 04 (Güvenlik / Altyapı):**
   _____
   _____
5. **Aksiyon 05 (Güvenlik / Altyapı):**
   _____
   _____
6. **Aksiyon 06 (Güvenlik / Altyapı):**
   _____
   _____
7. **Aksiyon 07 (Güvenlik / Altyapı):**
   _____
   _____
8. **Aksiyon 08 (Güvenlik / Altyapı):**
   _____
   _____
9. **Aksiyon 09 (Güvenlik / Altyapı):**
   _____
   _____
10. **Aksiyon 10 (Güvenlik / Altyapı):**
    _____
    _____

D) Dönüşüm ve Kontrol Takip Matrisi (Öncesi / Sonrası)

Güvenlik ve DR süreçlerinin standartlaşma öncesi ve sonrasındaki periyodik durum takibi:

Referans alınan **image_ce1605.png** denetim tablosundaki kurumsal hedeflere göre süreç şu şekilde işletilmektedir:

Kontrol Kriteri	Önce (Mevcut Durum)	Sonra (Hedeflenen Süreç)	Kanıt / Operasyonel Not
Token rotasyonu	TBD (Ölçülebilir veya Tanımlı Değil)	**Planlı:** API anahtarları belirli periyotlarla otomatik yenilenir.	Kod blokları temizlendi, env seviyesine çekildi.
Restore testi	TBD (Hiç Denenmedi)	**Aylık:** Alınan yedeklerin geri yükleme senaryoları simüle edilir.	Canlı ortam klonlanarak veri bütünlüğü doğrulandı.
_____	_____	_____	_____

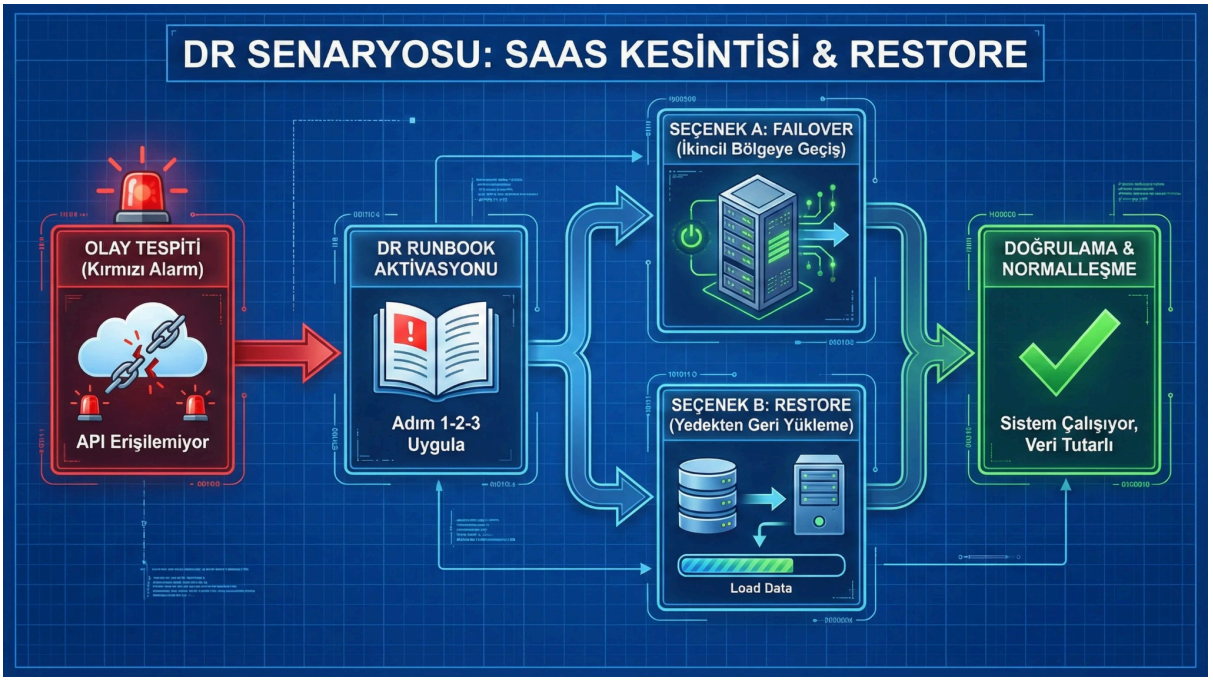
E) Nasıl Uygulanır? (5 Altın Kural)

1. **Sorumluluk Sınırlarını Net Çizin (SaaS vs Self-Hosted):** Headless CMS'i dışarıdan bir servis olarak alıyorsanız (Strapi Cloud, Contentful vb.), altyapı güvenliği ve sunucu ayakta kalma sorumluluğu servis sağlayıcıdadır. Ancak verilerin dışarı aktarılması, webhook güvenliği ve kullanıcı rolleri tamamen sizin ekibinizin sorumluluğundadır. Kendi sunucunuzda barındırıyorsanız (Self-hosted), veri tabanı yedekliliği ve sunucu güvenliği (OS updates) de listenize eklenmelidir.
2. **Yedek Kapsamını 3 Katmanlı Kurun:** Yalnızca yazılan metinleri yedeklemek kriz anında sistemi kurtarmaya yetmez. Yedekleme planınız; ham içerikleri (content), içerik modellerini ve veri tabanı ilişkilerini (schema) ve CMS'e ait tüm sistem/kullanıcı ayarlarını (settings) eş zamanlı olarak kapsamalıdır.
3. **"Geri Yüklenmeyen Yedek, Alınmamış Demektir" Prensibini Unutmayın:** Otomatik yedekleme script'lerinin hatasız çalışıyor görünmesi sizi yanıltmasın. Ayda en az bir kez, alınan güncel bir yedek dosyasını tamamen boş, izole bir test sunucusuna ayağa kaldırarak verilerin ve medya köprülerinin eksiksiz çalıştığını (Restore Testi) resmi olarak doğrulayın.
4. **Token Ömürlerini Sınırlandırın ve Rotasyona Alın:** Frontend katmanının Headless CMS API'leri ile konuşmasını sağlayan statik erişim anahtarlarını (Bearer Tokens) sonsuza kadar açık bırakmayın. Kritik token'lar için periyodik rotasyon planı hazırlayarak eski anahtarların sızma riskine karşı otomatik olarak deaktif edilmesini sağlayın.
5. **DR Runbook'u Teknik Olmayan Ekiplerin de Anlayabileceği Netlikte Yazın:** Büyük bir kesinti veya veri ihlali anında teknik ekipler panik yapabilir. Felaket Kurtarma Kılavuzunu (Runbook); kimin hangi komutu çalıştıracağını, müşterilere veya marka paydaşlarına hangi iletişim şablonuyla bilgi verileceğini (iletişim planı) adım adım, açık ve emir-komuta zincirine uygun şekilde dökümante edin.

Deliverables (Teslim Edilecek Çıktılar)

- **Sorumluluk Matrisi (Vendor vs Ekip):** CMS sağlayıcısı ile kurum içi teknik ekibin güvenlik ve operasyonel görev dağılımını ayıran RACI tablosu.
- **Backup Kapsam Dokümanı + Retention Politikası:** Yedeklenecek sistem katmanlarını, yedek frekansını ve eski yedeklerin ne kadar süreyle saklanacağını (retention) belirleyen saklama politikası.
- **Disaster Recovery Runbook + İletişim Planı:** Kriz anında uygulanacak teknik adımları, sistem ayağa kaldırma komutlarını ve paydaş bilgilendirme protokollerini içeren acil durum kılavuzu.
- **Tatbikat Takvimi + Postmortem Şablonu:** Yıllık DR simülasyon takvimi ve olası bir kriz atlatıldıktan sonra hatadan ders çıkarmak amacıyla kullanılacak teknik kök neden analiz (postmortem) şablonu.

Teknik liderler ve siber güvenlik sorumlularının altyapı güvenliğini ve iş sürekliliğini denetlemeleri için tasarlanmış, 1200x1200px kare formatında yüksek çözünürlüklü bir kurumsal DR checklist kartı. Koyu antrasit ve siber güvenlik temalı derin grafit tonlarındaki arka plan üzerinde, canlı mor ve neon turuncu renkte stratejik uyarı panelleri bulunuyor. Kartın üzerinde; "Rol Bazlı Yetki (RBAC) Kontrolü", "Gizli Token Rotasyon Takvimi", "3 Katmanlı Backup Kapsamı (Content+Schema)" ve "Aylık Canlı Restore Tatbikatı" adımları, yanlarında parlayan neon yeşili siber onay ikonları içeren son derece scannable ve kurumsal bir liste tasarımıyla sergileniyor.



Headless CMS altyapısında meydana gelebilecek olası bir sunucu çökmesi veya veri bozulması anında devreye giren otomatik yedek devralma (failover) ve canlı veriyi geri yükleme (restore) süreçlerini canlandıran, 1920x1080px Full HD çözünürlükte tasarlanmış teknik bir DR akış şeması. Minimalist gece siyahı bir zemin üzerinde, sol tarafta yer alan "Aktif CMS Altyapısı" üzerinde kırmızı renkli bir kesinti simülasyonu oluştuğunda, sistem algılayıcılarının asenkron olarak ortadaki güvenli "Yedek Depolama Katmanı (S3/Cloud)" düğümüne mor oklarla nasıl sinyal gönderdiği gösteriliyor. Sağ tarafta ise verinin sırasıyla Şema, İçerik ve Ayarlar olarak izole bir test cluster'ına yüklenip saniyeler içinde yeni "Canlı Frontend" hattına pürüzsüzce aktarılması süreci parlak altın sarısı ve elektrik mavisi hatlarla "clarity at a glance" felsefesine uygun olarak modellenmiştir.