Misafir Wi-Fi Captive Portal & Loglama KVKK Checklist Şablonu — Yazılım / Guest Wi-Fi (v1.0)

Asset Amaç: Bu asset, otel misafir Wi-Fi süreçlerini KVKK ve veri güvenliği perspektifiyle standardize eder: karşılama ekranı (*captive portal*) aydınlatması, kimlik doğrulama yöntemleri, minimum log veri seti, misafir/çalışan/yönetim ağ ayrımı ve yönetici paneli erişim güvenliği kontrol noktalarını netleştirir. Logların kapsamını ve erişim yetkilerini sınırlandırarak olası denetim ve siber olay (*incident*) anlarında teknik savunmayı güçlendirir. Sahada hızla uygulanabilir, düşük panik seviyeli bir denetim listesi sunar.

Kim Kullanır?: Otel BT/Network Ekipleri, Otel Operasyon Yöneticileri ve Bilgi Güvenliği/KVKK Sorumluları.

Nasıl Kullanılır?

1. Captive portal karşılama ekranını ve misafir giriş yöntemlerini (Oda No, Pasaport/TCKN, SMS) checklist kıstaslarına göre gözden geçirin.
2. Log veri setini veri minimizasyonu prensibiyle sınırlandırın; veri saklama (*retention*) ve Rol Bazlı Erişim Kontrolü (RBAC) yetkilerini tanımlayın.
3. Ağ segmentasyonunu (Misafir, Çalışan, Yönetim) uygulayın; admin panel erişimlerini MFA ve IP kısıtlamaları ile sıkılaştırıp simülasyon provasını gerçekleştirin.

TEMPLATE — Misafir Wi-Fi & Captive Portal KVKK Denetim Matrisi

1) Ölçüm & Önceliklendirme Checklist'i

Otel Wi-Fi altyapısının yasal düzenlemelere ve ağ güvenlik standartlarına uygunluğunu doğrulayan kontrol seti:

- [ ] **Captive Portal Aydınlatması Aktif:** Karşılama ekranında Kişisel Verilerin İşlenmesine İlişkin Aydınlatma Metni görünür ve erişilebilir şekilde yerleştirildi mi?
- [ ] **Mobil Uyumlu Kısa Özet Metin:** Aydınlatma metninin özet hali mobil ekranlarda okunabilir UX formatında tasarlandı mı?
- [ ] **Detaylı Metin Bağlantısı Eklendi:** Tam metne yönlendiren köprü bağlantısı (*link*) giriş butonunun hemen üzerinde belirgin şekilde yer alıyor mu?
- [ ] **Minimum Veri İle Login Yöntemi:** Kimlik doğrulama yöntemi elzem verilerle (Örn: Oda No + Doğum Yılı veya SMS verification) sınırlandırıldı mı?
- [ ] **Brute Force & Bot Koruması (Rate Limit):** Otomatik deneme/saldırı girişlerine karşı istek sınırlama (*rate limit*) ve IP engelleme kuralları aktif edildi mi?
- [ ] **Minimum Log Seti Tanımlandı:** Tutulan oturum logları sadece yasal zorunluluk kapsamındaki alanlarla (login_timestamp, logout_timestamp, local_ip, mac_address, assigned_public_ip, ssid) sınırlandırıldı mı?
- [ ] **Gereksiz Trafik ve İçerik Logları Kapalı:** Kullanıcıların gezindiği web sitelerinin detaylı URL, içerik ve paket loglarının tutulması kapatıldı mı?
- [ ] **Log Maskeleme ve PII Minimizasyonu:** Veri tabanında saklanan kişisel veriler (*PII*) ve erişim logları üzerinde anonimleştirme/maskeleme teknikleri uygulandı mı?
- [ ] **Log Saklama ve Rotasyon Politikası (Retention):** 5651 Sayılı Kanun ve KVKK gereksinimlerine uygun saklama süresi (Örn: 2 yıl) ve otomatik imha/rotasyon mekanizması kuruldu mı?

- [ ] **Rol Bazlı Log Erişimi (RBAC):** Ağ erişim loglarına yetkisiz personelin erişimi engellendi; erişim yetkileri sadece BT/Siber Güvenlik sorumluları ile sınırlandırıldı mı?
- [ ] **Ağ Segmentasyonu Yapıldı (VLAN / SSID):** Misafir ağı (*Guest Wi-Fi*), personel ağı (*Staff*) ve operasyonel sistemler (*PMS/POS*) fiziksel veya mantıksal (VLAN) olarak tamamen ayrıldı mı?
- [ ] **İç Sistemlere Erişim Engellendi (Deny Rules):** Misafir ağından otel veritabanlarına, PMS/POS sunucularına ve yönetim cihazlarına erişimi kesen güvenlik duvarı (*firewall*) kuralları yazıldı mı?
- [ ] **Yönetim Ağı Ayrıldı & IP Allowlist Kuruldu:** Ağ cihazları ve Wi-Fi denetleyicilerinin (*Controller*) yönetim arayüzleri ayrı bir yönetim VLAN'ına alınıp yalnızca tanımlı IP adreslerine (*allowlist*) açıldı mı?
- [ ] **Admin Panel Güvenliği (MFA & Audit Log):** Ağ yönetim panellerinde Çok Faktörlü Kimlik Doğrulama (MFA) zorunlu kılındı ve yönetici işlem kayıtları (*admin audit log*) aktif edildi mi?
- [ ] **Sözleşme ve Politika Versiyonlaması:** Captive portalda yayınlanan aydınlatma ve rıza metinlerinde yapılan her değişiklik versiyon numarasıyla (Örn: v1.0 $\rightarrow$ v1.1) kayıt altına alınıyor mu?

2) Problem $\rightarrow$ Kök Neden $\rightarrow$ Çözüm Matrisi

Misafir Wi-Fi altyapılarında karşılaşılan güvenlik ihlalleri ve teknik çözüm adımları:

Problem	Kök Neden	Çözüm
Misafir Wi-Fi ağına bağlanan cihazlar otel iç sistemlerine ve PMS/POS cihazlarına erişebiliyor	Ağ segmentasyonunun (VLAN/SSID) yapılmamış olması veya güvenlik duvarı erişim engelleme (*deny*) kurallarının eksikliği	Ayrı Guest VLAN yapılandırması + Güvenlik duvarında iç ağlara tüm erişimleri engelleyen katı kurallar (*deny rules*) + Yönetim ağı izolasyonu
Log dosyalarında kullanıcıların tüm web trafiği, arama geçmişi ve detay paketleri saklanıyor	Wi-Fi Controller ve Syslog sunucularında varsayılan geniş kapsamlı loglama ayarlarının açık kalması	Trafik detay loglarının kapatılması + Minimum yasal log seti kurgusu + Süresi dolan veriler için otomatik rotasyon/saklama (*retention*) kuralı
Ağ yönetim paneline yetkisiz kişiler veya iç ağdan herkes erişim denemesi yapabiliyor	Admin paneli erişimlerinde MFA ve IP kısıtlaması (*allowlist*) bulunmaması	Yönetim paneline MFA zorunluluğu + Statik IP allowlist kısıtlaması + RBAC yetkilendirmesi + Yönetici işlem logları (*admin audit*)

3) 14 Günlük Wi-Fi Güvenlik & KVKK Entegrasyon Sprint Planı

- **Gün 1: Wi-Fi Altyapı & Akış Envanteri:** Otel bünyesindeki tüm erişim noktaları (*AP*), Wi-Fi denetleyicileri, aktif SSID'ler, mevcut captive portal ve log sunucu mimarisi haritalandırılır.
- **Gün 2: Captive Portal UX & Aydınlatma Tasarımı:** Karşılama ekranı arayüzü mobil cihazlara uyumlu hale getirilir; kısa aydınlatma özet metni ve tam metin bağlantısı konumlandırılır.
- **Gün 3: Login Sadeleştirme & Rate Limit:** Giriş adımları veri minimizasyonuna göre (Oda No + TCKN/Pasaport veya SMS) düzenlenir; brute force saldırılarına karşı istek sınırlama (*rate limit*) kurgulanır.
- **Gün 4: Minimum Log Seti Yapılandırması:** Syslog sunucusunda yalnızca yasal zorunlulukta yer alan bağlantı parametrelerinin (timestamp, IP, MAC, SSID) saklanacağı şema kilitlenir.
- **Gün 5: Trafik Detay Loglarının Kapatılması:** Kullanıcıların veri gizliliğini ihlal edebilecek gereksiz paket analizi, web URL ve içerik loglama özellikleri pasife alınır.
- **Gün 6: Log Saklama (Retention) & İmha Tasarımı:** Log verilerinin yasal süre boyunca saklanmasını ve süresi dolan kayıtların otomatik silinmesini sağlayan rotasyon mimarisi kurulur.
- **Gün 7: Log Erişim RBAC & Audit Yapılandırması:** Log veritabanına erişimler yalnızca BT lideri ile sınırlandırılır ve log okuma/indirme hareketleri izlenebilir audit kaydına bağlanır.
- **Gün 8: Ağ Segmentasyonu (VLAN & SSID Ayrımı):** Misafir Wi-Fi (*Guest*), Personel (*Staff*) ve Operasyonel (*POS/PMS/IoT*) ağlar farklı VLAN ve subnet'lere ayrılır.
- **Gün 9: Güvenlik Duvarı Kural Tasarımı (Firewall Deny Rules):** Guest VLAN'dan otel sunucu bloklarına, yazıcılara ve operasyonel ağlara giden tüm veri trafiği güvenlik duvarında engellenir.
- **Gün 10: Yönetim Ağı İzolasyonu & Allowlist:** Ağ cihazları yönetim arayüzleri ayrı bir "Management VLAN" grubuna alınarak sadece belirli teknik IP'lerin erişimine açılır.
- **Gün 11: Admin Panel MFA & Yetki Temizliği:** Tüm ağ denetleyici ve firewall admin panellerinde Çok Faktörlü Kimlik Doğrulama (MFA) aktif edilir; eski/pasif hesaplar silinir.
- **Gün 12: Güvenlik Provası & Testler:** Misafir ağından iç ağlara sızma denemeleri, log paketleme bütünlüğü (*log bundle*) ve yetkisiz erişim simülasyonları gerçekleştirilir.
- **Gün 13: Dokümantasyon & Versiyonlama:** Yeni ağ mimarisi, erişim politikaları ve captive portal metin versiyonları kurumsal dokümantasyona işlenir.
- **Gün 14: Kapanış Raporu & Yıllık Yenileme Planı:** Sprint çıktıları yönetim raporuna dönüştürülür ve 365 günde bir tekrarlanacak periyodik denetim takvimi kilitlenir.

4) Öncesi / Sonrası Operasyonel KPI Tablosu

Misafir Wi-Fi KVKK uyumlaştırma ve altyapı sıkılaştırma çalışmasının performans çıktıları:

KPI Metriği	Önce (Eski Yapı)	Sonra (Sıkılaştırılmış Uyum Hedefi)	Stratejik Açıklama

Captive portal login başarı oranı	Düşük (Karmaşık formlar)	↑ **Artar** *(Hızlı ve Sade UX)*	Veri minimizasyonu ve sade arayüz sayesinde misafirlerin ağa bağlanma başarısı yükselir.
Misafir ağından iç sistem erişim denemesi	Riskli (Erişim Açık)	**0 (Kesin İzolasyon)**	Güvenlik duvarı engelleme kuralları ile misafir ağının otel verilerine erişim riski sıfırlanır.
Log verilerine erişim yetkili kişi sayısı	Geniş / Belirsiz	**Sadece Yetkili BT Sorumluları (RBAC)**	Log dosyalarına erişim rol bazlı kısıtlanarak veri sızıntısı riski ortadan kaldırılır.
Log retention / rotasyon uyumu	%0 – %40 (Düzensiz saklama)	**%100** *(Yasal ve Otomatik Rotasyon)*	Loglar yasal süre boyunca saklanır, süresi dolanlar sistemden otomatik imha edilir.
Siber olay (*incident*) analiz süresi	Günler alıyor / İmkânsız	**< 30 Dakika** *(Net ve Aranabilir Log)*	Standart ve temiz log seti sayesinde güvenlik olayları anında analiz edilip raporlanır.

5) Nasıl Uygulanır? (5 Wi-Fi Ağ Güvenliği Kuralı)

1. **Captive Portal Login Ekranında Çapraz Rıza İstemeyin:** Misafirin Wi-Fi hizmetinden faydalanabilmesi için "Pazarlama E-postası / SMS Almak İstiyorum" kutucuğunu işaretlemesini zorunlu tutmayın. Wi-Fi erişimini pazarlama onayına şart koşan kurgular KVKK açısından geçersiz rıza sayılır.
2. **Kullanıcı İzolasyonunu (*Client Isolation*) Aktif Edin:** Misafir Wi-Fi erişim noktalarında (*Access Point*) "Client Isolation" özelliğini açın. Bu sayede aynı Wi-Fi ağına bağlı iki farklı misafir cihazının birbirinin ağ trafiğini dinlemesini veya cihazlar arası yetkisiz bağlantı kurmasını engelleyin.
3. **Log Sunucusu Zaman Senkronizasyonunu (NTP) Sabitleyin:** Logların yasal denetimlerde ve adli adımlarda geçerli delil sayılabilmesi için tüm ağ cihazlarının, firewall'un ve syslog sunucusunun ortak bir Ağ Zaman Protokolü (*NTP Server*) üzerinden milisaniye hassasiyetinde senkronize olmasını sağlayın.
4. **Captive Portal Metinlerini Çok Dilli ve Versiyonlu Yönetin:** Otel misafir yelpazesine uygun olarak aydınlatma metinlerini Türkçe, İngilizce, Almanca ve Rusça dillerinde sunun. Her dildeki metin revizyonunu veritabanında versiyon numarası ve tarih etiketiyle arşivleyin.

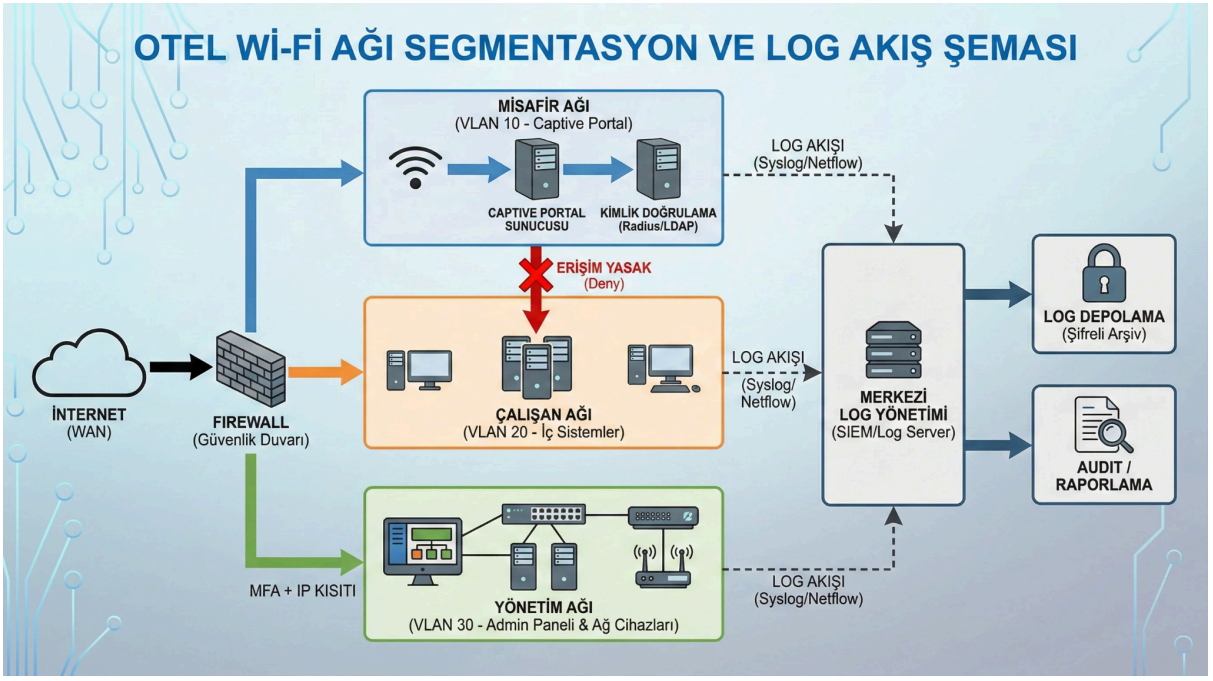
5. **Yönetim Arayüzlerini Asla İnternete Açmayın:** Wi-Fi denetleyicisi, firewall veya switch yönetim panellerini dış internete (*Public IP*) doğrudan açmayın. Uzaktan erişim gereksinimlerinde yalnızca şifreli VPN bağlantısı ve MFA doğrulaması sonrasında erişim izni verin.

Deliverables (Teslim Edilecek Çıktılar)

- **Captive Portal UX Mockup & Metin Seti:** Mobil uyumlu karşılama ekranı tel kafes (*wireframe*) tasarımı ve çok dilli aydınlatma/rıza metinleri dosyası.
- **Minimum Log Seti Dokümanı & Yetki Matrisi:** Saklanacak log parametrelerini, erişim rollerini (RBAC) ve saklama/silme periyotlarını belirten teknik standart dökümanı.
- **Ağ Segmentasyon & VLAN Şeması (Guest / Staff / Management):** Misafir, çalışan, operasyon ve yönetim ağlarının izole mimarisini gösteren ağ topolojisi diyagramı.
- **Admin Panel Erişim Politikası:** Yönetim panellerinin MFA, IP allowlist ve audit log yapılandırma standartlarını içeren güvenlik prosedürü.
- **Wi-Fi Denetim Provası Raporu & Yıllık Refresh Planı:** Gerçekleştirilen güvenlik simülasyon çıktısı, sızma testi sonuçları ve 365 günlük periyodik denetim takvimi.

[Deliverables / Proof Card]

Otel BT liderleri, network uzmanları ve bilgi güvenliği yöneticileri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir teknik teslimat ve doğrulama kartı. Koyu antrasit ve siber mavi tonlarındaki kurumsal arka plan üzerinde, mobil cihaz ekranında sergilenen sade bir Captive Portal arayüz mockup'ı, ağ güvenlik kalkanı ve onay işaretleri yer alıyor. Kartın üzerinde; "Mobil Uyumlu Captive Portal UX", "Ağ Segmentasyon Politikası (VLAN)", "Minimum Log Seti Standardı" ve "MFA Korumalı Admin Paneli" teslimat başlıkları, şık ikonlar ve okunabilir görsel hiyerarşi ile sergileniyor.



[Diagram / Flow]

Otel misafir Wi-Fi altyapısında bir cihazın ağa bağlanma, Captive Portal aydınlatmasını onaylama, IP/MAC alma ve log verilerinin izole sunuculara aktarılma sürecini gösteren, 1920x1080px (16:9) Full HD çözünürlükte mimari akış diyagramı. Koyu gece mavisi zemin üzerinde, en soldaki "Misafir Cihazı (Guest Device)" kutusundan çıkan yön okları, "Captive Portal & Minimum Login (Oda No / SMS)" adımına geçiyor. Buradan ayrılan hatlar, üst tarafta güvenlik duvarı engel kuralıyla "İç Ağlara Erişim Engellendi (Deny Rules)" kırmızı alanına takılırken; alt tarafta yeşil ve turkuaz akış hatlarıyla "İzole Guest VLAN", "NTP Senkronlu Minimum Syslog Sunucusu" ve "RBAC Korumalı Log Arşivi" uç noktalarına bağlanarak "clarity at a glance" felsefesiyle şemalaştırılıyor.