Sızma Testi Kapsam Belirleme ve Yetkilendirme Formu

Form No: ST-KF-___ | **Sürüm:** 1.0 | **Tarih:**

Gizlilik Sınıfı: ☐ Çok Gizli ☐ Gizli ☐ Hizmete Özel ☐ Kurum İçi

1. Doküman Kontrolü

Alan	Bilgi
Proje / Talep Adı	
Proje Referans No	
Sözleşme / Sipariş No ve Tarihi	
Hazırlayan	
Kurum Onaylayan	

2. Taraf Bilgileri

2.1 Kurum (Test Yaptıran / Sistem Sahibi)

Alan	Bilgi
Ticari Unvan / Kurum Adı	
Vergi Dairesi / No – MERSİS No	
Adres	
Yetkili Temsilci (Ad, Unvan)	
Proje Sorumlusu (Ad, Unvan, Telefon, E-posta)	
Bilgi Güvenliği / BT Sorumlusu (Ad, Telefon, E-posta)	
Kişisel Verileri Koruma Sorumlusu (Ad, Telefon, E-posta)	
Kurumun Tabi Olduğu Düzenleyici Otorite	☐ BDDK ☐ SPK ☐ BTK ☐ EPDK ☐ Sağlık Bakanlığı ☐ Kamu Kurumu ☐ Diğer: ____
Kritik Altyapı / Temel ve Önemli Hizmet Kapsamında mı?	☐ Evet ☐ Hayır ☐ Bilinmiyor

2.2 Test Hizmeti Sağlayıcı

Alan	Bilgi
Ticari Unvan / Ad-Soyad	
Vergi Dairesi / No – MERSİS No	
Adres	
Yetkili Temsilci	
Proje Yöneticisi (Ad, Telefon, E-posta)	
Siber Güvenlik Başkanlığı ve ilgili mevzuat uyarınca gereken yetki / sertifika / belge (varsa) ve numarası	
Kalite ve Güvenlik Belgeleri	☐ ISO 27001 ☐ ISO 9001 ☐ Diğer: ____
Mesleki Sorumluluk / Siber Sigorta	☐ Var (Poliçe No, Limit: ____) ☐ Yok
Alt Yüklenici Kullanılacak mı?	☐ Evet (Bölüm 16'ya bakınız) ☐ Hayır

2.3 Test Ekibi

Ad Soyad	Rol	T.C. Kimlik No / Pasaport No	Sertifikalar (OSCP, CEH, GPEN vb.)	Gizlilik Taahhüdü İmzalandı mı?
				☐ Evet ☐ Hayır
				☐ Evet ☐ Hayır

3. Yasal Dayanak ve Yetkilendirme Beyanı

3.1 Dayanak Mevzuat

Bu form ve test faaliyetleri aşağıdaki mevzuat çerçevesinde değerlendirilir. İlgili sektöre özel düzenlemeler ayrıca eklenmelidir.

- **5237 sayılı Türk Ceza Kanunu** m. 243 (Bilişim sistemine girme), m. 244 (Sistemi engelleme, bozma, verileri yok etme veya değiştirme), m. 135–136 (Kişisel verilerin kaydedilmesi ve hukuka aykırı olarak verme / ele geçirme): Yazılı ve yetkili izin bulunmaksızın yapılacak test faaliyetleri suç teşkil edebilir. İşbu form, test faaliyetlerinin kurum tarafından açık ve yazılı olarak yetkilendirildiğinin delilidir.
- **6698 sayılı Kişisel Verilerin Korunması Kanunu** (KVKK) ve ikincil mevzuat: Veri güvenliğine ilişkin yükümlülükler (m. 12), aydınlatma ve işleme şartları (m. 4, 5, 10), yurt dışına aktarım (m. 9).
- **7545 sayılı Siber Güvenlik Kanunu** ve Siber Güvenlik Başkanlığı'nca çıkarılan yönetmelik, tebliğ ve standartlar: Siber güvenlik hizmet sağlayıcılarına ilişkin yetkilendirme, belgelendirme ve denetim hükümleri.
- **5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun** ve **5809 sayılı Elektronik Haberleşme Kanunu**: Log, erişim ve haberleşme gizliliğine ilişkin hükümler.
- **6102 sayılı Türk Ticaret Kanunu** (ticari sır, sır saklama), **6098 sayılı Türk Borçlar Kanunu** (sözleşme, sorumluluk), **5846 sayılı Fikir ve Sanat Eserleri Kanunu** (rapor ve yazılım telif hakları).
- **Sektörel düzenlemeler** (uygulanan işaretlenmelidir): ☐ 5411 sayılı Bankacılık Kanunu ve BDDK Bilgi Sistemleri Yönetmeliği ☐ SPK düzenlemeleri ☐ BTK düzenlemeleri ☐ EPDK düzenlemeleri ☐ Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi ☐ PCI DSS ☐ Diğer: ____

3.2 Kurum Yetkilendirme Beyanı

Kurum olarak;

1. Bu formda **Kapsam Dahilinde** olarak listelenen tüm sistem, ağ, uygulama ve varlıkların sahibi veya yasal işletici olduğumuzu, bunlar üzerinde test yaptırmaya yetkili olduğumuzu,
2. Bu varlıkların üçüncü taraflarca barındırılması veya işletilmesi hâlinde (bulut, hosting, SaaS, dış kaynak hizmet sağlayıcılar), ilgili üçüncü taraftan **yazılı izin** aldığımızı veya almakla yükümlü olduğumuzu ve bu izinlerin Ek-2'de sunulduğunu,
3. Test Hizmeti Sağlayıcı'nın ve test ekibinin, bu formda belirtilen kapsam, zaman aralığı ve kurallar dâhilinde, tarafımızca yetkilendirildiğini,
4. Kapsam dışı bırakılan varlıklara yönelik herhangi bir faaliyetin yetkisiz olduğunu,
5. Test faaliyetlerinin kişisel verilere erişim ihtimali taşıdığı ve bu hususta KVKK kapsamındaki yükümlülüklerimizin tarafımızca değerlendirildiğini

beyan ve kabul ederiz.

3.3 Test Hizmeti Sağlayıcı Beyanı

Test Hizmeti Sağlayıcı olarak;

1. Yalnızca bu formda yazılı kapsam, yöntem ve zaman aralığı içinde hareket edeceğimizi,
2. Test faaliyetlerini yürürlükteki mevzuata ve bu forma uygun olarak gerçekleştireceğimizi,

3. Hizmetin sunulması için mevzuatın aradığı yetki, belge ve sertifikalara sahip olduğumuzu veya bu yükümlülüğe tabi olmadığımızı,
4. Test ekibimizin kişisel veri ve gizli bilgilere ilişkin gizlilik taahhüdü verdiğini,
5. Kapsam dışı sistemlere erişim tespit edilmesi hâlinde derhâl durup Kurum'a bildirimde bulunacağımızı

beyan ve taahhüt ederiz.

4. Testin Amacı ve Hedefleri

4.1 Test Amacı (uygun olanları işaretleyin)

☐ Güvenlik açığı tespiti ☐ Yasal / düzenleyici uyumluluk (Dayanak: ____) ☐ Yeni sistemin devreye alma öncesi doğrulaması ☐ Değişiklik sonrası doğrulama ☐ Tehdit simülasyonu / Red Team ☐ Önceki bulguların yeniden testi ☐ Diğer: ____

4.2 Beklenen Çıktı ve Başarı Kriterleri:

_____

_____

_____

_____

5. Test Türü ve Yaklaşımı

Boyut	Seçenekler
Bilgi Düzeyi	☐ Black Box ☐ Grey Box ☐ White Box
Konum	☐ Dış Ağ (İnternetten) ☐ İç Ağ ☐ Uzaktan (VPN)
Bilgilendirme	☐ Duyurulu (BT/SOC bilgilendirilmiş) ☐ Duyurusuz (Sınırlı kişi bilgili)
Yaklaşım	☐ Zafiyet Taraması ☐ Sızma Testi ☐ Red Team ☐ Purple Team

Test Edilecek Alanlar:

☐ Web Uygulaması ☐ Mobil Uygulama (iOS / Android) ☐ API / Web Servisi ☐ Dış Ağ Altyapısı ☐ İç Ağ Altyapısı ☐ Kablosuz Ağ ☐ Active Directory / Kimlik Altyapısı ☐ Bulut Altyapısı ☐ Sunucu / İşletim Sistemi ☐ Veritabanı ☐ Güvenlik Duvarı / Ağ Cihazı ☐ IoT / Gömülü Sistem ☐ OT / SCADA / Endüstriyel Sistem ☐ Fiziksel Güvenlik ☐ Kaynak Kod İncelemesi ☐ Yapılandırma İncelemesi

Referans Metodoloji / Standartlar: ☐ OWASP (Web / API / Mobile) ☐ PTES ☐ NIST SP 800-115 ☐ OSSTMM ☐ MITRE ATT&CK ☐ CVSS ☐ Diğer: ____

6. Kapsam Dâhilindeki Varlıklar

No	Varlık Adı	IP / Alan Adı / URL / Ağ Aralığı	Ortam	Barındırma Yeri	Kritiklik	Kişisel Veri İçerir mi?
1			☐ Üretim ☐ Test ☐ Geliştirme	☐ Kurum ☐ Bulut ☐ 3. Taraf	☐ Yüksek ☐ Orta ☐ Düşük	☐ Evet ☐ Hayır
2			☐ Üretim ☐ Test ☐ Geliştirme	☐ Kurum ☐ Bulut ☐ 3. Taraf	☐ Yüksek ☐ Orta ☐ Düşük	☐ Evet ☐ Hayır
3			☐ Üretim ☐ Test ☐ Geliştirme	☐ Kurum ☐ Bulut ☐ 3. Taraf	☐ Yüksek ☐ Orta ☐ Düşük	☐ Evet ☐ Hayır

Test İçin Sağlanacak Hesaplar / Erişimler:

Hesap / Rol	Yetki Düzeyi	Sağlanma Şekli	Geçerlilik Süresi

7. Kapsam Dışı Varlıklar ve Yasaklı Faaliyetler

7.1 Kapsam Dışı Varlıklar

No	Varlık / IP / Alan Adı	Kapsam Dışı Bırakılma Gerekçesi
1		
2		
3		
4		

7.2 Yasaklı Faaliyetler (Aksi Açıkça Yetkilendirilmedikçe)

Faaliyet	Yetki Durumu
Hizmet engelleme saldırıları (DoS / DDoS, kaynak tüketme, stres testi)	☐ Yasak ☐ İzinli (Koşul: ____)
Üretim verisinin silinmesi, değiştirilmesi veya bozulması	☐ Yasak ☐ İzinli (Koşul: ____)
Üretim verisinin test ortamı dışına çıkarılması / kopyalanması	☐ Yasak ☐ Sınırlı (Bölüm 9)
Sosyal mühendislik (kurum çalışanlarına yönelik)	☐ Yasak ☐ İzinli (Hedef Liste: ____)
Fiziksel sızma	☐ Yasak ☐ İzinli (Konum: ____)
Exploit çalıştırma (sistem kararlılığını etkileyebilecek)	☐ Yasak ☐ Sadece Test Ortamında ☐ İzinli
Parola kırma / brute force	☐ Yasak ☐ Sınırlı (Hesap kilitleme politikası dikkate alınarak)
Kalıcılık (persistence) sağlama, arka kapı bırakma	☐ Yasak ☐ İzinli (Sonrasında temizlenmek kaydıyla)
Yanal hareket (lateral movement) ve yetki yükseltme	☐ Yasak ☐ İzinli (Sınır: ____)
Üçüncü taraf sistemlere (kapsam dışı) erişim veya saldırı	**Kesinlikle yasak**
Kurum çalışanlarının / müşterilerinin kişisel hesaplarına erişim	**Kesinlikle yasak**
Elde edilen erişim, veri veya bilginin test amacı dışında kullanılması	**Kesinlikle yasak**

8. Test Kuralları

Başlık	Belirleme
Test Başlangıç – Bitiş Tarihi	
İzin Verilen Saat Aralığı	☐ 7/24 ☐ Mesai Saatleri ☐ Mesai Dışı: ____ – ____
Bakım / Değişiklik Dondurma Dönemleri	
Kaçınılacak Kritik İş Dönemleri	
Testin Gerçekleştirileceği Kaynak IP Adresleri	
Test Gerçekleştirilecek Fiziksel / Uzaktan Lokasyon	
Kullanılacak Ana Araçlar	
Tarama Hızı / Eşzamanlı Bağlantı Sınırı	
Yedekleme Alındı mı? (Üretim sistemleri için)	☐ Evet ☐ Hayır ☐ Gerekli Değil
Test Öncesi Sistem Sağlık Kontrolü	☐ Yapıldı ☐ Gerekli Değil
Kritik Zafiyet Tespitinde Anında Bildirim	☐ Evet (Süre: ____ saat içinde)
Test Sırasında Yapılan Tüm İşlemlerin Loglanması	☐ Evet (Log saklama süresi: ____)
Test Sonrası Temizlik (dosya, hesap, arka kapı, geçici yapılandırma)	☐ Test Hizmeti Sağlayıcı yükümlüdür

9. Kişisel Veri ve Gizli Bilgilerin Korunması

Konu	Belirleme
Test sırasında kişisel veriye erişim ihtimali	☐ Yok ☐ Düşük ☐ Yüksek
Özel nitelikli kişisel veri bulunuyor mu?	☐ Evet ☐ Hayır ☐ Bilinmiyor
Test Hizmeti Sağlayıcı'nın rolü	☐ Veri İşleyen ☐ Bağımsız Veri Sorumlusu
Veri İşleme Sözleşmesi / Ek Protokol	☐ Ek-4 olarak imzalandı

Taraflarca kabul edilen veri koruma ilkeleri:

1. Test faaliyetlerinde kişisel veri işleme **asgari düzeyde** tutulur. Zafiyetin kanıtlanması için gerekli olan en az veri örneği alınır; toplu veri çekimi yapılmaz.
2. Rapor ve ekran görüntülerinde kişisel veriler (T.C. kimlik no, ad-soyad, telefon, adres, kart no, sağlık verisi, parola vb.) **maskelenir**.
3. Test sırasında elde edilen veri, kanıt ve loglar şifreli ortamda saklanır; yalnızca yetkili test ekibi erişir.
4. Test sırasında elde edilen kimlik bilgileri (parola, token, anahtar) rapor dışında paylaşılmaz; rapor teslimi sonrasında ____ gün içinde güvenli şekilde imha edilir.
5. Veri ihlali şüphesi veya kontrolsüz kişisel veri erişimi tespitinde Test Hizmeti Sağlayıcı Kurum'u **derhâl** bilgilendirir; KVKK uyarınca Kurum'un Kişisel Verileri Koruma Kurulu'na bildirim süreci (72 saat) Kurum sorumluluğundadır.
6. Test faaliyetleri sonucunda elde edilen veriler, test amacı dışında kullanılamaz, üçüncü kişilere aktarılamaz, yurt dışına çıkarılamaz.
7. Test sonrası kanıt ve veri saklama süresi: ____ gün. Süre sonunda tutanak karşılığında imha edilir.

10. İletişim ve Acil Durum Yönetimi

Rol	Ad Soyad	Telefon (7/24)	E-posta
Kurum Proje Sorumlusu			
Kurum BT / Bilgi Güvenliği Acil Durum Kişisi			
Kurum SOC / SIEM İzleme Birimi			
Test Hizmeti Sağlayıcı Proje Yöneticisi			
Test Hizmeti Sağlayıcı Acil Durum Kişisi			

Acil Durum ve Durdurma Prosedürü:

1. Kurum, bir sistemde beklenmeyen etki, hizmet kesintisi veya gerçek bir siber saldırı şüphesi görürse testi **derhâl durdurma** yetkisine sahiptir. Test Hizmeti Sağlayıcı talep üzerine ___ dakika içinde faaliyetleri durdurur.
2. Test Hizmeti Sağlayıcı beklenmeyen bir etki, sistem kararsızlığı veya kapsam dışına taşma fark ederse faaliyeti durdurur ve ___ dakika içinde Kurum'u bilgilendirir.
3. Kurum SOC birimi, test kaynak IP adreslerini bilir ve test faaliyeti ile gerçek saldırıları ayırt eder (duyurusuz testlerde bu bilgi sınırlı kişilerde tutulur).
4. Kritik ve yüksek seviyeli zafiyetler rapor beklenmeksizin ___ saat içinde sözlü / yazılı olarak bildirilir.
5. Gerçek bir siber olay tespit edilirse tarafların yasal bildirim yükümlülükleri (SOME, Siber Güvenlik Başkanlığı, KVKK, sektörel otorite) Kurum tarafından yönetilir.

11. Zaman Planı

Aşama	Başlangıç	Bitiş	Sorumlu
Kapsam Netleştirme ve Onay			
Bilgi Toplama / Keşif			
Zafiyet Tespiti			
Sızma / Sömürü			
Raporlama			
Rapor Sunumu / Kapanış Toplantısı			
Düzeltme Dönemi			
Yeniden Test (Retest)			

12. Teslimatlar ve Raporlama

Teslimat	Dil	Format	Teslim Tarihi
Yönetici Özeti Raporu	☐ TR ☐ EN	☐ PDF ☐ Diğer	
Teknik Detay Raporu (kanıtlar, adım adım yeniden üretim)	☐ TR ☐ EN	☐ PDF ☐ Diğer	
Düzeltme Önerileri / Aksiyon Planı	☐ TR ☐ EN	☐ PDF ☐ Diğer	
Yeniden Test Raporu	☐ TR ☐ EN	☐ PDF ☐ Diğer	
Kapanış Sunumu	☐ TR ☐ EN	☐ Sunum	

Raporlama İlkeleri:

- Risk derecelendirmesi: ☐ CVSS v3.1 ☐ CVSS v4.0 ☐ Kurumsal Risk Matrisi
- Rapor, bulguları kritik / yüksek / orta / düşük / bilgilendirme seviyelerinde sınıflandırır.
- Rapor yalnızca Kurum'un belirlediği alıcılara, şifreli ve güvenli kanal üzerinden iletilir.
- Yeniden test hakkı: ☐ Dahil (Süre: ____ gün) ☐ Ayrıca ücretlendirilir ☐ Yok
- Raporlar, Test Hizmeti Sağlayıcı tarafından Kurum'un yazılı izni olmaksızın üçüncü kişilerle paylaşılamaz, referans olarak kullanılamaz.

13. Gizlilik ve Bilgi Güvenliği

1. Taraflar, bu form kapsamında öğrendikleri her türlü ticari sır, teknik bilgi, zafiyet bilgisi, kişisel veri ve diğer gizli bilgiyi gizli tutmayı, yalnızca bu proje amacıyla kullanmayı kabul eder.
2. Gizlilik yükümlülüğü, test sona erdikten sonra ____ yıl süreyle devam eder; kişisel veri ve ticari sırlar bakımından süresiz geçerlidir.
3. Test ekibine ait tüm cihazlar güncel, uç nokta koruması aktif, disk şifrelemeli olacaktır. Test verileri, kurum sistemleri dışında kontrolsüz ortamlarda (kişisel bulut, kişisel e-posta, mesajlaşma uygulamaları) saklanamaz veya iletilemez.
4. Tespit edilen zafiyetler, Kurum'un yazılı izni olmaksızın üçüncü kişilere, ilgili üreticilere, kamuya veya medyaya açıklanamaz.

14. Sorumluluk, Sigorta ve Tazminat

Konu	Belirleme
Test kaynaklı hizmet kesintisi riskinin Kurum tarafından kabulü	☐ Kabul edilmiştir ☐ Kabul edilmemiştir
Test Hizmeti Sağlayıcı'nın kusurlu / kapsam dışı eylemlerinden doğan zararlar	Test Hizmeti Sağlayıcı sorumludur
Sorumluluk Üst Limiti	____ TL / ☐ Sözleşme bedeli kadar ☐ Sınırsız (kast ve ağır kusur hariç sınır uygulanamaz)
Üretim sistemleri için Kurum yedekleme sorumluluğu	Kurum, test öncesi yedek almakla yükümlüdür

15. Fikri Mülkiyet ve Rapor Mülkiyeti

1. Test sonucunda hazırlanan raporların ve elde edilen bulguların mülkiyeti ve kullanım hakkı **Kurum'a** aittir.
2. Test Hizmeti Sağlayıcı'nın önceden geliştirdiği araç, metodoloji, şablon ve know-how'u Test Hizmeti Sağlayıcı'ya ait kalır.
3. Test sırasında oluşturulan özel exploit kodları, betikler ve kanıt dosyaları Kurum'un talebi hâlinde teslim edilir veya imha edilir.

16. Alt Yüklenici Kullanımı

Alt Yüklenici Unvanı	Yürüteceği İş	Yurt İçi / Yurt Dışı	Kurum Onayı
		☐ Yurt İçi ☐ Yurt Dışı	☐ Onaylandı ☐ Reddedildi

17. Mevzuata Uyum Kontrol Listesi

No	Kontrol	Durum	Sorumlu
1	Test Hizmeti Sağlayıcı'nın gerekli yetki / belge / sertifika durumu doğrulandı	☐ Evet ☐ Hayır ☐ Gerekli Değil	
2	Tüm kapsam varlıkları için Kurum'un sahiplik / işletme yetkisi doğrulandı	☐ Evet ☐ Hayır	
3	Üçüncü taraf (bulut, hosting, SaaS) yazılı izinleri alındı	☐ Evet ☐ Hayır ☐ Gerekli Değil	
4	Test ekibi için gizlilik taahhütleri imzalandı	☐ Evet ☐ Hayır	
5	NDA imzalandı	☐ Evet ☐ Hayır	
6	KVKK veri işleme sözleşmesi / protokolü imzalandı	☐ Evet ☐ Hayır ☐ Gerekli Değil	
7	Sektörel düzenleyici otoriteye bildirim / izin gerekliliği değerlendirildi	☐ Evet ☐ Hayır ☐ Gerekli Değil	
8	İlgili iç birimler ve SOC bilgilendirildi	☐ Evet ☐ Hayır ☐ Gerekli Değil	
9	Üretim sistemleri için yedek alındı ve geri dönüş planı hazırlandı	☐ Evet ☐ Hayır ☐ Gerekli Değil	
10	Acil durum iletişim zinciri test edildi	☐ Evet ☐ Hayır	
11	Kamu kurumları için: ilgili rehber ve standartlara (ör. Bilgi ve İletişim Güvenliği Rehberi) uyum değerlendirildi	☐ Evet ☐ Hayır ☐ Gerekli Değil	

18. Değişiklik Yönetimi

Bu formda belirlenen kapsam, kurallar veya zaman aralığında yapılacak her değişiklik, taraflarca **yazılı olarak** ve Kurum'un yetkili onayıyla yapılır. Sözlü ve e-posta ile yapılan kapsam değişiklikleri, ancak form eki olarak imzalanıp kayda alındığında geçerlidir.

Değişiklik No	Tarih	Değişiklik Açıklaması	Kurum Onayı	Sağlayıcı Onayı

19. Onay ve İmzalar

İşbu form ve ekleri okunmuş, anlaşılmış ve yukarıdaki kapsam, kurallar, beyan ve taahhütler kabul edilmiştir. Kurum onayı alınmadan hiçbir test faaliyeti başlatılamaz.

	Kurum	**Test Hizmeti Sağlayıcı**
Unvan		
Ad Soyad		
Görev		
Tarih		
İmza / Kaşe		

Ek Onaylar

Rol	Ad Soyad	Tarih	İmza
Bilgi Güvenliği / BT Müdürü			
Kişisel Verileri Koruma Sorumlusu			

Ekler

- **Ek-1:** Detaylı Varlık Listesi (IP aralıkları, alan adları, uygulama listesi)
- **Ek-2:** Üçüncü Taraf Yazılı İzinleri (bulut, hosting, SaaS sağlayıcıları)
- **Ek-3:** Gizlilik Sözleşmesi (NDA)
- **Ek-4:** Kişisel Veri İşleme Sözleşmesi / Protokolü
- **Ek-5:** Test Ekibi Gizlilik ve Etik Taahhütnamesi
- **Ek-6:** İmza Yetkisi Belgeleri (imza sirküleri, yetki belgesi)
- **Ek-7:** Test Hizmeti Sağlayıcı Yetki, Belge ve Sertifikaları
- **Ek-8:** Kaynak IP Adresleri ve Test Hesapları Listesi

EK-1: Detaylı Varlık Listesi

Proje Referans No: _____ | Tarih: //_____ | Form Sürümü: ____

EK-1.A Ağ ve Altyapı Varlıkları

No	Varlık Adı	IP Adresi / Aralığı (CIDR)	Konum (DMZ / İç Ağ / Bulut)	İşletim Sistemi / Cihaz Tipi	Sahip Birim	Test Türü	Kurum Paraf
1						☐ Dış ☐ İç	
2						☐ Dış ☐ İç	
3						☐ Dış ☐ İç	
4						☐ Dış ☐ İç	
5						☐ Dış ☐ İç	
6						☐ Dış ☐ İç	
7						☐ Dış ☐ İç	
8						☐ Dış ☐ İç	
9						☐ Dış ☐ İç	
10						☐ Dış ☐ İç	

EK-1.B Web Uygulamaları, API ve Alan Adları

No	Uygulama / Servis Adı	URL / Alan Adı	Teknoloji / Çatı	Ortam	Kimlik Doğrulama Türü	Roller	Barındırma / Sağlayıcı	Kurum Paraf
1				☐ Üretim ☐ Test				
2				☐ Üretim ☐ Test				
3				☐ Üretim ☐ Test				
4				☐ Üretim ☐ Test				
5				☐ Üretim ☐ Test				
6				☐ Üretim ☐ Test				
7				☐ Üretim ☐ Test				

EK-1.C Mobil Uygulamalar

No	Uygulama Adı	Platform	Sürüm	Mağaza Bağlantısı / Paket Adı	Test Edilecek Backend	Kurum Paraf
1		☐ iOS ☐ Android				
2		☐ iOS ☐ Android				

EK-1.D Kablosuz Ağlar, Fiziksel Lokasyonlar ve Diğer

No	Varlık / Lokasyon	SSID / Adres / Tanım	Test Türü	Özel Kısıtlar	Kurum Paraf
1					
2					

EK-1.E Kapsam Dışı Bırakılan Varlıklar

No	Varlık / IP / Alan Adı	Gerekçe
1		
2		

Listeyi Hazırlayan: _____ Tarih: //_____ Kurum Onayı (Ad, İmza): _____

EK-2: Üçüncü Taraf Yazılı Test İzin Belgesi

Tarih:

Sayın _____ (Üçüncü Taraf Hizmet Sağlayıcı Unvanı)

Konu: Sızma Testi İzin Talebi ve Onayı

1. _____ (Kurum Unvanı) olarak, _____ (Proje Referans No) numaralı proje kapsamında, tarafınızca barındırılan / işletilen / sağlanan aşağıdaki sistemler üzerinde, _____ (Test Hizmeti Sağlayıcı Unvanı) tarafından yetkilendirilmiş sızma testi gerçekleştirilmesi planlanmaktadır.

2. Test Edilecek Sistemler:

No	Hizmet / Sistem	IP / Alan Adı / Kaynak Kimliği	Hizmet Türü (IaaS/PaaS/SaaS)	Hesap / Abonelik No
1				
2				

3. Test Koşulları:

- Test Tarihleri:
- Saat Aralığı: ____ – ____
- Test Kaynak IP Adresleri: _____
- Test Türü: ☐ Dış Ağ ☐ Uygulama ☐ Yapılandırma ☐ Diğer: ____
- Hizmet engelleme (DoS/DDoS), kaynak tüketme ve diğer müşterilerin sistemlerini etkileyebilecek faaliyetler **yapılmayacaktır**.

4. İşbu talebin kabulü ile yukarıda belirtilen sistemler üzerinde, belirtilen kapsam, tarih ve koşullarla sınırlı olmak üzere sızma testi yapılmasına izin verdiğinizi, tarafınızca bu testin hukuka aykırı bir erişim veya saldırı olarak değerlendirilmeyeceğini ve sistemlerinizde bu faaliyetin tespiti hâlinde güvenlik/izleme ekiplerinizin bilgilendirileceğini kabul etmiş olursunuz.

Talep Eden Kurum Yetkilisi: Ad Soyad: _____ Unvan: _____ İmza/Kaşe: _____

ÜÇÜNCÜ TARAF ONAYI

☐ Test talebi yukarıdaki koşullarla **onaylanmıştır.** ☐ Test talebi **reddedilmiştir.** Gerekçe: _____ ☐ Test talebi aşağıdaki **değişiklik ve ek koşullarla** onaylanmıştır: _____

Onay Referans / Bilet No: _____ Onay Tarihi: //_____

Onaylayan Yetkili (Ad, Unvan): _____ İmza/Kaşe: _____

EK-3: Gizlilik Sözleşmesi

Sözleşme No: _____ | **Tarih:**

Madde 1 – Taraflar

1.1 Kurum ("Bilgi Veren"): Unvan: _____ Vergi Dairesi / No: _____ MERSİS No: _____ Adres: _____

1.2 Test Hizmeti Sağlayıcı ("Bilgi Alan"): Unvan / Ad Soyad: _____ Vergi Dairesi / No: _____ MERSİS No: _____ Adres: _____

Bu sözleşmede Kurum ve Test Hizmeti Sağlayıcı birlikte "Taraflar", ayrı ayrı "Taraf" olarak anılır. Sözleşmenin tarafları karşılıklı bilgi paylaşımı yapacak ise gizlilik yükümlülüğü karşılıklı olarak uygulanır.

Madde 2 – Amaç

Bu sözleşmenin amacı, Taraflar arasında _____ (Proje Referans No) numaralı **Sızma Testi ve Kapsam Belirleme Formu** çerçevesinde yürütülecek test faaliyetleri sırasında Tarafların edineceği gizli bilgilerin korunması, yetkisiz kişilerce öğrenilmesinin ve kullanılmasının önlenmesidir.

Madde 3 – Gizli Bilginin Tanımı

3.1 "Gizli Bilgi"; yazılı, sözlü, elektronik, görsel veya başka herhangi bir şekilde, doğrudan veya dolaylı olarak, test faaliyetlerinden önce, sırasında veya sonrasında paylaşılan, ifşa edilen veya erişilen ve aşağıdakileri kapsayan tüm bilgidir (kapsam sınırlayıcı değildir):

- Kurum'un ağ topolojisi, IP adresleri, alan adları, sistem mimarisi, kaynak kodu, yapılandırma dosyaları, kimlik bilgileri, şifreleme anahtarları, API anahtarları ve erişim belirteçleri,
- Test sürecinde tespit edilen tüm **güvenlik açıkları, zafiyetler, sömürü yöntemleri ve bunlara ilişkin bilgi ve kanıtlar**,
- Rapor, bulgu, ekran görüntüsü, log ve çıktılar,
- Kurum'un müşterilerine, çalışanlarına, iş ortaklarına ilişkin bilgiler ve **kişisel veriler** (özel nitelikli kişisel veriler dahil),
- Ticari sır niteliğindeki bilgiler, bankacılık sırrı, müşteri sırrı, finansal bilgiler, iş planları, ticari stratejiler,
- Bu sözleşmenin ve test çalışmasının varlığı ile içeriği.

3.2 Bilginin "gizli" ibaresi taşımaması, gizli bilgi niteliğini ortadan kaldırmaz.

Madde 4 – İstisnalar

Aşağıdaki bilgiler, ispatı Bilgi Alan'a ait olmak üzere gizli bilgi sayılmaz; ancak kişisel veriler ve bilgi güvenliği açısından hassas veriler bu istisnalardan **hiçbir koşulda** yararlanamaz:

- Bilgi Alan'ın ihlali olmaksızın kamuya mal olmuş bilgiler,
- Açıklama öncesinde Bilgi Alan'ın yasal yoldan, gizlilik yükümü olmaksızın elde ettiğini yazılı belgeyle ispatlayabildiği bilgiler,
- Bilgi Alan tarafından bağımsız olarak, Gizli Bilgi kullanılmaksızın geliştirilen bilgiler

Madde 5 – Yükümlülükler

Bilgi Alan;

5.1 Gizli Bilgi'yi yalnızca sözleşme amacıyla kullanacağını ve hiçbir koşulda kendi veya üçüncü kişilerin yararına ticari, rekabet veya başka amaçla kullanmayacağını,

5.2 Gizli Bilgi'yi kendi gizli bilgilerini koruduğu özenden az olmamak üzere, en az sektörde kabul görmüş bilgi güvenliği standartları düzeyinde koruyacağını,

5.3 Gizli Bilgi'ye erişimi, görev gereği erişmesi zorunlu **ve gizlilik taahhüdü imzalamış** çalışanlar/danışmanlarla ("Bilmesi Gereken İlkesi") sınırlandıracağını,

5.4 Gizli Bilgi'yi Bilgi Veren'in yazılı onayı olmaksızın alt yükleniciler dahil hiçbir üçüncü kişiye açıklamayacağını, onay verilmesi hâlinde alt yüklenicinin de bu sözleşmeyle en az aynı yükümlülüklere tabi tutulacağını ve alt yüklenicinin fiillerinden doğrudan sorumlu olacağını,

5.5 Gizli Bilgi'yi kopyalamayacağını, çoğaltmayacağını, yalnızca sözleşme amacının gerektirdiği ölçüde **şifreli ve kontrollü** ortamlarda saklayacağını; kişisel e-posta, kişisel bulut, kişisel mesajlaşma uygulaması gibi kontrolsüz ortamlarda tutmayacağını veya iletmeyeceğini,

5.6 Tespit edilen zafiyetleri; Bilgi Veren'in yazılı izni olmaksızın üçüncü kişilere, yazılım üreticilerine, kamuya, medyaya, sosyal medyaya, konferans veya yayınlara **açıklamayacağını ve referans olarak kullanmayacağını**,

5.7 Gizli Bilgi'nin yetkisiz açıklanması, kaybı, çalınması veya ihlal şüphesini **derhal, en geç 24 saat içinde** yazılı olarak Bilgi Veren'e bildireceğini, zararın azaltılması için gerekli tüm tedbirleri alacağını ve Bilgi Veren'le iş birliği yapacağını,

kabul, beyan ve taahhüt eder.

Madde 6 – Kişisel Verilerin Korunması

Gizli Bilgi içinde yer alan kişisel veriler bakımından 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil mevzuat hükümleri ile EK-4 **Kişisel Veri İşleme Sözleşmesi / Protokolü** hükümleri ayrıca uygulanır. Bu sözleşme ile EK-4 arasında çelişki olması hâlinde kişisel verilerin korunması bakımından EK-4 hükümleri önceliklidir.

Madde 7 – Mülkiyet, Hak Devri Yasağı ve İade / İmha

7.1 Gizli Bilgi üzerindeki tüm haklar Bilgi Veren'e aittir. Bu sözleşme, Bilgi Alan'a herhangi bir lisans, kullanım veya mülkiyet hakkı vermez.

7.2 Sözleşmenin sona ermesi, test faaliyetinin tamamlanması veya Bilgi Veren'in talebi hâlinde Bilgi Alan, elindeki tüm Gizli Bilgi'yi ve kopyalarını ___ iş günü içinde iade eder veya geri döndürülemez biçimde imha eder ve imhayı **EK-9 Veri İmha ve Hesap Kapatma Tutanağı** ile yazılı olarak belgeler.

7.3 Yasal saklama yükümlülüğü bulunan kayıtlar bu hükmün istisnasıdır; bu kayıtlar sözleşme hükümlerine tabi kalmaya devam eder.

Madde 8 – Süre

8.1 Bu sözleşme imza tarihinde yürürlüğe girer ve ilgili test faaliyetleri ile ilişkili tüm sözleşmesel yükümlülükler sona erdikten sonra da **____ (yazıyla: ____) yıl** boyunca yürürlükte kalır.

8.2 Kişisel veriler, ticari sırlar, bankacılık sırrı, müşteri sırrı ve güvenlik zafiyetlerine ilişkin bilgiler bakımından gizlilik yükümlülüğü **süresiz** devam eder.

Madde 9 – Cezai Şart ve Tazminat

9.1 Bilgi Alan'ın veya alt yüklenicileri ile çalışanlarının bu sözleşmenin gizlilik hükümlerini ihlal etmesi hâlinde, Bilgi Alan her bir ihlal için **____ TL (yazıyla: ____ Türk Lirası)** cezai şart ödemeyi kabul eder. (6098 sayılı Türk Borçlar Kanunu m. 179 ve devamı)

9.2 Cezai şart, Bilgi Veren'in ihlal sebebiyle uğradığı gerçek zararın tazminini talep hakkını ortadan kaldırmaz; cezai şartı aşan zarar için ayrıca tazminat talep edilebilir.

9.3 Taraflar, bu sözleşmenin ihlalinin 5237 sayılı Türk Ceza Kanunu'nun ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanmasına (m. 239), bilişim sistemi ve kişisel verilere ilişkin suçlara (m. 135-138, 243-244) ve ilgili diğer hükümlere göre ayrıca cezai ve hukuki sorumluluk doğurabileceğini bilmektedir.

Madde 10 – Hak Kaybı Olmaması, Devir ve Bölünebilirlik

10.1 Taraflardan birinin sözleşmeden doğan bir hakkını kullanmaması veya geç kullanması, o haktan feragat anlamına gelmez.

10.2 Bilgi Alan, bu sözleşmeden doğan hak ve yükümlülüklerini Bilgi Veren'in yazılı onayı olmadan devredemez.

10.3 Sözleşmenin herhangi bir hükmünün geçersiz sayılması, diğer hükümlerin geçerliliğini etkilemez.

Madde 11 – Uygulanacak Hukuk ve Yetkili Mahkeme

Bu sözleşme Türk hukukuna tabidir. Sözleşmeden doğacak uyuşmazlıklarda **Ankara (____) Mahkemeleri ve İcra Daireleri** yetkilidir.

Madde 12 – Yürürlük ve Nüsha

Bu sözleşme 12 maddeden ibaret olup, **//**_____ tarihinde, iki nüsha olarak düzenlenmiş ve Taraflarca imzalanmıştır.

	Bilgi Veren (Kurum)	**Bilgi Alan (Test Hizmeti Sağlayıcı)**
Unvan		
Ad Soyad		
Görev		
İmza / Kaşe		

EK-4: Kişisel Veri İşleme Sözleşmesi / Protokolü

Protokol No: _____ | **Tarih:** ……/……/……

Madde 1 – Taraflar ve Roller

Veri Sorumlusu ("Kurum"): Unvan: _____ Adres: _____ VERBİS Sicil No: _____

Veri İşleyen ("Test Hizmeti Sağlayıcı"): Unvan: _____ Adres: _____

Madde 2 – Dayanak ve Amaç

Bu protokol; 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK") m. 12, Kişisel Verileri Koruma Kurulu'nun düzenlemeleri ve Kişisel Verileri Koruma Kurumu'nca yayımlanan Kişisel Veri Güvenliği Rehberi çerçevesinde; _____ (Proje Referans No) numaralı sızma testi sırasında karşılaşılabilecek kişisel verilerin korunmasına ve işlenmesine ilişkin esasları belirler.

Madde 3 – Veri İşlemenin Konusu, Süresi, Türü ve Amacı

Konu	Belirleme
İşleme Konusu	Sızma testi sırasında test kapsamındaki sistemlerde bulunan kişisel verilere **tesadüfen veya zafiyetin kanıtlanması amacıyla** erişim
İşleme Amacı	Güvenlik açıklarının tespiti ve raporlanması. Başka hiçbir amaçla işlenemez.
İşleme Süresi	Test süresi + rapor teslimi + saklama süresi (EK-9 imha tarihine kadar), en fazla ____ gün
Veri Kategorileri	☐ Kimlik ☐ İletişim ☐ Müşteri İşlem ☐ Finansal ☐ Çalışan ☐ Sağlık ☐ Biyometrik ☐ Lokasyon ☐ Log / İşlem Güvenliği ☐ Diğer: ____
Özel Nitelikli Kişisel Veri	☐ Yok ☐ Var (Tür: ____)
İlgili Kişi Grupları	☐ Müşteriler ☐ Çalışanlar ☐ Ziyaretçiler ☐ Tedarikçi / İş Ortakları ☐ Diğer: ____
Veri Aktarımı	☐ Yok ☐ Yurt içi alt işleyene ☐ Yurt dışı (KVKK m. 9 uyarınca)

Madde 4 – Veri İşleyenin Yükümlülükleri

Test Hizmeti Sağlayıcı;

1. Kişisel verileri yalnızca Kurum'un yazılı talimatları ve bu protokol çerçevesinde, sızma testi amacıyla işler; kendi veya üçüncü kişilerin amaçları için kullanamaz.
2. **Veri minimizasyonu ilkesine** uyar; zafiyeti kanıtlamak için gerekli olan en az kayıt örneğini alır, toplu veri çekimi, tam veritabanı kopyası veya dışa aktarım yapmaz.
3. Rapor ve ekran görüntülerinde kişisel verileri (T.C. kimlik no, ad soyad, telefon, e-posta, adres, kart numarası, IBAN, sağlık verisi, parola vb.) **maskeler veya anonimleştirir**.
4. Veri güvenliğini sağlamak üzere KVKK m. 12 uyarınca uygun düzeyde teknik ve idari tedbirleri alır; en az şunları uygular:
    - Test cihazlarında disk şifreleme, güncel işletim sistemi, uç nokta koruma
    - Kanıt ve verilerin yalnızca şifreli ortamlarda saklanması
    - Erişimin yalnızca yetkili ve gizlilik taahhüdü vermiş test ekibi üyelerine sınırlandırılması, erişim kayıtlarının tutulması
    - Çok faktörlü kimlik doğrulama (mümkün olduğu ölçüde)
    - Verilerin kişisel cihaz, kişisel e-posta, kişisel bulut ve mesajlaşma uygulamalarında saklanmaması ve iletilmemesi
    - Rapor ve kanıtların yalnızca güvenli, şifreli kanal ile iletilmesi
5. Test ekibinin tüm üyelerinin gizlilik ve kişisel veri taahhüdü verdiğini garanti eder (EK-5).
6. Kişisel verileri Kurum'un yazılı onayı olmaksızın yurt dışına aktarmaz ve yurt dışında barındırılan sistemlerde saklamaz.
7. Kurum'un yazılı onayı olmadan alt işleyen kullanmaz; onay verilmesi hâlinde alt işleyene bu protokoldeki yükümlülükleri aynen yükler ve onun fiillerinden doğrudan sorumlu olur.
8. İlgili kişilerden gelen başvuruları (bilgi talebi, düzeltme, silme vb.) doğrudan yanıtlamaz; ____ saat içinde Kurum'a iletir.
9. Kişisel verilerin hukuka aykırı olarak ele geçirildiğini veya ele geçirilmiş olabileceğini öğrendiği anda, **derhal ve en geç 24 saat içinde** Kurum'a yazılı bildirimde bulunur; olayın kapsamı, etkilenen veri, olası sonuçlar ve alınan önlemler hakkında bilgi verir ve zararı azaltma çalışmalarına iştirak eder.
10. Kurum'un makul bir bildirimle talep etmesi hâlinde, bu protokole uyumu kanıtlayan bilgi ve belgeleri sunar, Kurum'un veya yetkilendirdiği denetçinin denetimine imkân tanır.

Madde 5 – Veri Sorumlusunun (Kurum) Yükümlülükleri

Kurum;

1. Test kapsamındaki sistemlerde işlenen kişisel veriler bakımından KVKK m. 10 uyarınca ilgili kişileri aydınlatma ve işleme şartlarını sağlama yükümlülüğünün kendisinde olduğunu,
2. Test faaliyetlerinin gerektirdiği ölçüde VERBİS ve veri işleme envanterini güncel tuttuğunu,
3. Veri ihlali hâlinde, KVKK m. 12/5 uyarınca ihlali **en kısa sürede ve en geç 72 saat içinde** Kişisel Verileri Koruma Kurulu'na ve gerekiyorsa ilgili kişilere bildirmekle yükümlü olduğunu (bildirim yükümlülüğü Kurum'a aittir)

kabul eder.

Madde 6 – Veri Saklama, İade ve İmha

6.1 Test ile ilgili elde edilen kişisel veriler, kanıtlar ve loglar, rapor tesliminden itibaren en geç ____ gün içinde ve her halükarda sözleşmenin sona ermesinde; Kurum'un talebi doğrultusunda iade edilir veya KVKK ile ilgili düzenlemelere uygun olarak **geri döndürülemez biçimde silinir, yok edilir veya anonim hâle getirilir.**

6.2 İmha işlemi **EK-9 Veri İmha ve Hesap Kapatma Tutanağı** ile belgelenir.

6.3 Yasal saklama yükümlülüğü bulunan kayıtlar, ilgili süre boyunca bu protokol hükümlerine tabi olarak korunur.

Madde 7 – Sorumluluk ve Cezai Şart

7.1 Veri İşleyen, bu protokolün ihlali sebebiyle Kurum'un ve ilgili kişilerin uğrayacağı zararlardan, idari para cezalarına ilişkin rücu haklarını da kapsayacak şekilde sorumludur.

7.2 Bu protokolün ihlali hâlinde Veri İşleyen, her bir ihlal için **____ TL** cezai şart öder. Bu tutar, ihlalden doğan gerçek zararın tazminini talep hakkını ortadan kaldırmaz.

7.3 Taraflar, kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilmesi veya ele geçirilmesinin 5237 sayılı Türk Ceza Kanunu m. 135, 136, 138 uyarınca ayrıca cezai sorumluluk doğurabileceğini kabul eder.

Madde 8 – Süre ve Yürürlük

Bu protokol imza tarihinde yürürlüğe girer, test sona erdikten ve EK-9 imha tutanağı düzenlendikten sonra da, kişisel veriye ilişkin yükümlülükler bakımından, verilerin tamamen imhasına kadar devam eder.

Madde 9 – Uyuşmazlık

Bu protokolden doğan uyuşmazlıklarda Türk hukuku uygulanır; **Ankara (____) Mahkemeleri ve İcra Daireleri** yetkilidir.

	Veri Sorumlusu (Kurum)	**Veri İşleyen (Test Hizmeti Sağlayıcı)**
Unvan		
Ad Soyad		
Görev		
Tarih		
İmza / Kaşe		

EK-5: Test Ekibi Gizlilik ve Etik Taahhütnamesi

Proje Referans No: _____ | Tarih: ……/……/……

Ad Soyad: _____ T.C. Kimlik No / Pasaport No: _____ Çalıştığı Kuruluş: _____ Görev: _____ Sertifikalar: _____

Yukarıda kimliği belirtilen kişi olarak;

A. Kapsam ve Yetki

1. Yalnızca Kurum tarafından yazılı olarak onaylanan kapsam, kurallar ve zaman aralığı içinde test faaliyetinde bulunacağımı, **kapsam dışı sistemlere hiçbir şekilde müdahale etmeyeceğimi**,
2. Yazılı yetki bulunmayan hiçbir sisteme, hesaba, ağa veya fiziksel alana erişmeyeceğimi,
3. Kapsam dışına çıktığımı fark etmem hâlinde derhal durup Proje Yöneticisi'ne bildireceğimi,
4. Test faaliyetlerimin 5237 sayılı Türk Ceza Kanunu'nun bilişim suçlarına ilişkin hükümleri) bakımından, yalnızca Kurum'un yazılı yetkilendirmesi dahilinde hukuka uygun olabileceğinin bilincinde olduğumu,

B. Gizlilik ve Veri Koruma

5. Test sırasında edindiğim her türlü bilgiyi (zafiyetler, sistem bilgileri, kimlik bilgileri, kişisel veriler, ticari sırlar dahil) gizli tutacağımı; hizmet sona erse dahi süresiz olarak koruyacağımı,
6. Bu bilgileri yalnızca test amacıyla kullanacağımı, başka hiçbir amaçla (ticari, kişisel, akademik, yayın, sosyal medya vb.) kullanmayacağımı ve üçüncü kişilerle paylaşmayacağımı,
7. Kişisel verilere erişmem hâlinde 6698 sayılı KVKK ve EK-4 hükümlerine uyacağımı, **yalnızca gerekli asgari miktarda** veri alacağımı, raporlarda verileri maskeleyeceğimi,
8. Veri ve kanıtları yalnızca şifreli ve yetkilendirilmiş cihazlarda saklayacağımı, kişisel cihaz, kişisel e-posta, kişisel bulut ve mesajlaşma uygulamalarında tutmayacağımı,
9. Test sonunda tüm veri, kanıt ve kimlik bilgilerini talimat doğrultusunda güvenli biçimde imha edeceğimi,

C. Etik Kurallar

10. Kurum sistemlerine, verilerine veya hizmetlerine **zarar vermeyeceğimi**, hizmet kesintisine yol açabilecek faaliyetleri yetkilendirme olmaksızın yapmayacağımı,
11. Elde ettiğim erişimi yalnızca yetkilendirilmiş sınırlar içinde kullanacağımı, **arka kapı, kalıcı yazılım veya kontrolsüz değişiklik bırakmayacağımı**,
12. Elde ettiğim erişimi, veriyi veya bilgiyi kendi, işverenim veya üçüncü kişiler lehine **kullanmayacağımı**,
13. Yazılı izin olmaksızın tespit ettiğim zafiyetleri üreticilere, kamuya veya üçüncü kişilere açıklamayacağımı,
14. Bu taahhütlere aykırı davranışımın hukuki, cezai ve tazminat sorumluluğu doğuracağını, çalıştığım kuruluşun sözleşme ve disiplin hükümlerine tabi olacağımı

beyan ve taahhüt ederim.

İmza: _____ Tarih: ……/……/……

EK-6: İmza Yetkisi Belgeleri

EK-6.A Kurum İmza Yetkisi

Ad Soyad	Unvan / Görev	Yetki Türü	Yetki Sınırı	Belge Tür ve Tarihi	Belge No
		☐ Münferit ☐ Müşterek		☐ İmza Sirküleri ☐ Yönetim Kurulu Kararı ☐ Vekâletname ☐ Görevlendirme	
		☐ Münferit ☐ Müşterek		☐ İmza Sirküleri ☐ Yönetim Kurulu Kararı ☐ Vekâletname ☐ Görevlendirme	

EK-6.B Test Hizmeti Sağlayıcı İmza Yetkisi

Ad Soyad	Unvan / Görev	Yetki Türü	Yetki Sınırı	Belge Tür ve Tarihi	Belge No
		☐ Münferit ☐ Müşterek		☐ İmza Sirküleri ☐ Yönetim Kurulu Kararı ☐ Vekâletname ☐ Görevlendirme	
		☐ Münferit ☐ Müşterek		☐ İmza Sirküleri ☐ Yönetim Kurulu Kararı ☐ Vekâletname ☐ Görevlendirme	

EK-6.C Beyan

Yukarıda adı geçen kişilerin, bu formu ve ekleri taraf kuruluşlar adına imzalamaya, bağlayıcı beyanda bulunmaya ve bu form kapsamında sistemleri test ettirmeye/test etmeye **yetkili olduklarını** beyan ederiz.

Kurum Yetkilisi: Ad Soyad: _____ İmza/Kaşe: _____ Tarih: ……/……/……

Test Hizmeti Sağlayıcı Yetkilisi: Ad Soyad: _____ İmza/Kaşe: _____ Tarih: ……/……/……

Eklenen Belgeler: ☐ İmza sirküleri ☐ Ticaret sicil gazetesi ☐ Yetki belgesi / vekâletname ☐ Yönetim kurulu kararı ☐ Görevlendirme yazısı ☐ Diğer: _____

EK-7: Test Hizmeti Sağlayıcı Yetki, Belge ve Sertifikaları

EK-7.A Kurumsal Yetki ve Belgeler

Belge / Yetki	Veren Kurum	Belge No	Geçerlilik Başlangıç	Geçerlilik Bitiş	Kapsam	Ekte?
ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi						☐
ISO 9001 Kalite Yönetim Sistemi						☐
Diğer						☐
Ticaret Sicil Gazetesi / Faaliyet Belgesi						☐
Vergi Levhası						☐

EK-7.B Ekip Sertifikaları

Ad Soyad	Sertifika (OSCP, OSWE, GPEN, CEH, CISSP, eWPT vb.)	Sertifika No	Veren Kurum	Geçerlilik Bitiş	Ekte?
					☐
					☐
					☐

EK-8: Test Kaynak IP Adresleri, Test Hesapları ve Araç Listesi

EK-8.A Test Kaynak IP Adresleri

No	Kaynak IP / Aralık	Konum / Sağlayıcı	Kullanan Test Uzmanı	Kullanım Tarih Aralığı	Kurum SOC'a Bildirildi
1					☐ Evet ☐ Gerekli Değil
2					☐ Evet ☐ Gerekli Değil
3					☐ Evet ☐ Gerekli Değil

EK-8.B Test Hesapları (Grey / White Box)

No	Hesap Adı / Kullanıcı Kimliği	Sistem / Uygulama	Rol / Yetki Düzeyi	Sağlanma Tarihi	Geçerlilik Bitiş	Sağlayan Birim	Kapatma Tarihi
1							
2							
3							

EK-8.C Kullanılacak Ana Araçlar

Araç Adı	Sürüm	Amaç	Lisans (Açık Kaynak / Ticari)	Kurum Onayı
				☐ Onaylandı ☐ Reddedildi
				☐ Onaylandı ☐ Reddedildi
				☐ Onaylandı ☐ Reddedildi

Not: Listede yer almayan, sistem kararlılığını etkileyebilecek veya zararlı yazılım niteliği taşıyan araç ve exploit kodları, Kurum'un önceden yazılı onayı olmadan kullanılamaz. Kullanılan araçların güncel, lisanslı ve güvenli kaynaklardan temin edilmiş olması Test Hizmeti Sağlayıcı sorumluluğundadır.

Hazırlayan (Test Hizmeti Sağlayıcı): _____ **Onaylayan (Kurum):** _____ **Tarih:** ……/……/……

EK-9: Veri İmha ve Hesap Kapatma Tutanağı

Proje Referans No: _____ | **Tutanak Tarihi:** ……/……/…… | **Test Dönemi:** ……/……/…… – ……/……/……

EK-9.A İmha Edilen Veri ve Kayıtlar

No	Veri / Kayıt Türü	Saklama Ortamı	İmha Yöntemi	Kişisel Veri İçeriyor mu?	İmha Tarihi	İmhayı Yapan
1	Test kanıtları (ekran görüntüsü, çıktı)		☐ Güvenli silme ☐ Fiziksel imha ☐ Diğer	☐ Evet ☐ Hayır		
2	Ağ trafiği kayıtları (pcap vb.)		☐ Güvenli silme ☐ Fiziksel imha ☐ Diğer	☐ Evet ☐ Hayır		
3	Elde edilen kimlik bilgileri / parolalar / anahtarlar		☐ Güvenli silme ☐ Fiziksel imha ☐ Diğer	☐ Evet ☐ Hayır		
4	Çıkarılan veri örnekleri		☐ Güvenli silme ☐ Fiziksel imha ☐ Diğer	☐ Evet ☐ Hayır		
5	Taslak ve çalışma raporları		☐ Güvenli silme ☐ Fiziksel imha ☐ Diğer	☐ Evet ☐ Hayır		
6	Yedekler ve kopyalar		☐ Güvenli silme ☐ Fiziksel imha ☐ Diğer	☐ Evet ☐ Hayır		

EK-9.B Hesap, Erişim ve Yapılandırma Kapatma

Kontrol	Yapıldı mı?	Tarih	Sorumlu
Test hesapları devre dışı bırakıldı / silindi	☐ Evet ☐ Gerekli Değil		
Test hesaplarının parolaları değiştirildi	☐ Evet ☐ Gerekli Değil		
Test sırasında oluşturulan hesaplar, dosyalar, görevler, kayıt defteri girdileri silindi	☐ Evet ☐ Gerekli Değil		
Arka kapı, web shell, kalıcı bileşen bırakılmadığı doğrulandı	☐ Evet ☐ Gerekli Değil		
Test kaynak IP'leri için tanımlanan güvenlik duvarı / WAF izinleri kaldırıldı	☐ Evet ☐ Gerekli Değil		
VPN ve uzaktan erişim yetkileri kaldırıldı	☐ Evet ☐ Gerekli Değil		

Kontrol	Yapıldı mı?	Tarih	Sorumlu
Test sırasında yapılan geçici yapılandırma değişiklikleri geri alındı	☐ Evet ☐ Gerekli Değil		
Test sırasında ele geçirilen kimlik bilgileri/anahtarlar Kurum tarafından yenilendi	☐ Evet ☐ Gerekli Değil		
Test ekibi fiziksel erişim kartları / anahtarları iade edildi	☐ Evet ☐ Gerekli Değil		

EK-9.C Beyan

Test Hizmeti Sağlayıcı olarak; bu projede elde edilen tüm gizli bilgi, kişisel veri ve kanıtların yukarıda belirtilen şekilde, geri döndürülemez biçimde imha edildiğini, hiçbir kopyasının tarafımızda, ekip üyelerimizde veya alt yüklenicilerimizde bulunmadığını, yukarıdaki kapatma işlemlerinin yapıldığını beyan ederiz.

Kurum olarak; yukarıdaki hesap ve erişim kapatma işlemlerinin kendi sistemlerimizde yapıldığını kabul ederiz.

	Test Hizmeti Sağlayıcı	**Kurum**
Ad Soyad		
Görev		
Tarih		
İmza / Kaşe		