



**YENİ NESİL AKARYAKIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA
AİT ÖKC TSM'LERİNİN
BAŞVURU, TEST, DENETİM VE ONAY
TEKNİK KILAVUZU**

Sürüm 2.0

30 ARALIK 2021

İÇİNDEKİLER

GİRİŞ	4
1. Amaç ve Kapsam	4
BÖLÜM I	6
YENİ NESİL AKARYAKIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM GÜVENLİK GEREKSİNİMLERİ	6
2. Kritik Varlıklar ve Aktörler	6
2.1 Kritik Varlıklar	6
2.1.1 Birincil Varlıklar.....	6
2.1.2 İkincil Varlıklar	7
2.2 Aktörler.....	7
2.2.1 Yetkili Kullanıcılar	7
2.2.2 Yetkisiz Kullanıcılar (Hacker, Siber Terörist, vb.).....	7
2.2.3 Teçhizat ve Yazılımlar.....	8
2.2.4 Çevresel Koşullar	8
3. Sistem Güvenliği, İş Sürekliliği, Felaket Kurtarma ve Olay Müdahale	8
4. Kullanılan Donanımların Güvenliği.....	8
5. Kullanılan Yazılımların Güvenliği.....	8
6. Güvenlik Denetimi	9
BÖLÜM II.....	10
YENİ NESİL AKARKAYIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM SİSTEM GEREKSİNİMLERİ.....	10
7. ÖKC TSM'lerinin Desteklemesi Gereken Standartlar.....	10
7.1 Uluslararası Standartlar	10
7.2 Ulusal Standartlar	11
8. ÖKC TSM Başvuru, Test, Denetim ve Onay Süreçleri.....	11
9. Sistemlerin Münhasırlığı.....	11
10. ÖKC TSM'leri Sorumluluk Dağılımı	14
11. Mükellef, YN Pompa ÖKC, ÖKC TSM'leri ve BİM İletişimi.....	15
12. YN Pompa ÖKC Mesajlarının Yönetimi	16
13. Risk Yönetimi Esasları.....	16
14. Değişiklik Yönetimi.....	17
15. Denetim İzlerinin Oluşturulması.....	17

16. Anahtar Yönetim Süreçleri ve Veri Güvenliği	19
17. Yazılım Güvenliği ve Sorumluluğu	20
18. İş Sürekliliği Yönetimi.....	20
19. Dış Hizmet Alımı.....	23
20. Personel Gereksinimleri.....	24
20.1 Network & Network Güvenlik Grubu:	24
20.2 Sistem ve Database Grubu:.....	24
20.3 Sistem ve Terminal Operasyon Grubu:	25
20.4 Uygulama Geliştirme Grubu:	25
21. ÖKC TSM'lerinin Periyodik Denetimi.....	25
22. Başkanlık Uyarı Mekanizmaları	26
BÖLÜM III.....	27
YENİ NESİL AKARYAKIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC	
TSM'LERİ ONAY VE TEST BAŞVURU AKIŞLARI	27
23. Onay ve Test Başvuru Yönetimi	27
23.1 ÖKC TSM Başvurusunda Sağlanacak Belgeler	27
23.2 ÖKC TSM Denetim ve Onay Süreçleri.....	28
23.3 Dış Hizmet Sağlayıcı ÖKC TSM Denetim ve Onay Süreçleri.....	29
23.4 Onay Denetimi Sonrasında Test Başvuruları ve Gerçek Ortama Geçiş	30
BÖLÜM IV	31
ÖKC TSM'LERİNDE GERÇEKLEŞTİRİLECEK DENETİM FAALİYETLERİ	31
24. ÖKC TSM'lerinde Gerçekleştirilecek Onay Denetiminin Kapsamı.....	31
24.1 ÖKC TSM'leri Bilgi Sistemleri Denetimi	31
24.2 ÖKC TSM'leri Güvenli Haberleşme Denetimi	32
25. ÖKC TSM'lerinde Gerçekleştirilecek Periyodik Denetiminin Kapsamı.....	33
26. ÖKC TSM Denetimine İlişkin Düzenlenen Raporların Formatı	34
27. KILAVUZ EKLERİ.....	35
EK-1: Denetim Mektubu Oluşturulurken Metinde Değiştirilmesi Gereken Hususlar:	35
EK-2: ÖKC TSM Başvuru Formu.....	36
EK-3 : “ÖKC TSM Onay Denetim Raporu Formatı”	40
EK-4A : “ÖKC TSM Periyodik Denetim Raporu Formatı	41
EK-4B: “ÖKC TSM Güncelleme Denetimi Rapor Formatı.....	42

GİRİŞ

1. Amaç ve Kapsam

Bu Kılavuz Gelir İdaresi Başkanlığının (Başkanlık) Yeni Nesil Akaryakıt Pompa ÖKC (YN Pompa ÖKC) projesine dahil olan ve ÖKC TSM kurmak isteyen ya da ÖKC TSM hizmetini bir Dış Hizmet Sağlayıcı (DHS)'dan temin etmek isteyen ÖKC Üreticileri için hazırlanmıştır. Kılavuzda ÖKC TSM'leri (TSM) ibaresi aksi belirtilmediği müddetçe DHS'yi de kapsamakta olup TSM ile DHS birlikte kastedilmektedir.

ÖKC TSM hizmeti kurarak ya da bir dış hizmet sağlayıcıdan alarak cihazlarını yönetmek ve BİM ile iletişim kurmak isteyen ÖKC Üreticileri bu Kılavuzu rehber edinerek teknik konularını yönetebilecektir. Bu Kılavuz, ÖKC TSM kurmak, işletmek, yönetmek ve denetlemek isteyenler için hazırlanan “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Teknik Kılavuzu” esas alınarak hazırlanmıştır. “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Teknik Kılavuzu”nda yer almayan bazı detayları açıklamak amacıyla yazılmış olan bu Kılavuz, tek başına değerlendirilmemeli, konu ile ilgili diğer dokümanlarla birlikte değerlendirilmelidir.

ÖKC TSM'sinin gerekli şartları haiz olup olmadığının tespiti için gerekli onay denetimi, 13/01/2010 tarihli ve 27461 sayılı Resmi Gazete’de yayımlanan “Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik” (BSDHY) kapsamında yetkilendirilmiş veya izin verilmiş Bağımsız Denetim Kuruluşlarınca (BDK) veya TÜBİTAK tarafından yerinde yapılmak zorundadır.

Onay denetimi, bu Kılavuzda açıklanan; “Bilgi Sistemi Denetim Adımları” ve “Güvenli Haberleşme Denetim Adımları” olmak üzere iki aşamadan oluşur.

ÖKC TSM'sinin onay aldığı durumda; onay yazısını takip eden 3 yıllık süre sonunda ve takip eden her 3 yılda bir defa olmak üzere; “Bilgi Sistemi Denetim Adımları”, “Bilgi Sistemi Denetimi” ismi altında tekrar edilir. Bilgi Sistemi Denetimine ilişkin usul ve esaslara bu Kılavuzda detaylı olarak yer verilmiştir.

“Güvenli Haberleşme Denetim Adımları” onay sürecine münhasıran uygulanır. Ancak Başkanlık, GMP’ dokümanlarında gerçekleştirilecek değişikliklere istinaden bu denetimlerin tekrar edilmesini talep edebilir.

Bu Kılavuzun I. Bölümünde, ÖKC TSM’lerinin sahip olması gereken **güvenlik gereksinimleri** açıklanmaktadır. Bu bölümde yer alan gereksinimler ÖKC TSM topolojilerinden bağımsız olarak Yeni Nesil Akaryakıt Pompa ÖKC Teknik Kılavuzu ve GMP dokümanı temel alınarak hazırlanmıştır. (Bu bölüm, hassas verinin yetkisiz kişilerin eline geçmesini engellemeyi, verinin hem bilgisayar sistemlerinde, hem saklama ortamlarında, hem de ağ üzerinde gönderici ve alıcı arasında taşınırken yetkisiz erişimlerden korunması, gizliliği, bütünlüğü ve sürekliliği ile alakalı hususlar için güvenlik gereksinimlerinin belirlenmesi amacı ile oluşturulmuştur.)

Bu Kılavuzun II. Bölümünde, ÖKC TSM’lerinin kurması gereken veri merkezlerinin, uygulamalarının sahip olması gereken **sistem gereksinimleri** detaylandırılmaktadır. Bu bölümde Başkanlık, ÖKC Üreticileri, ÖKC TSM’leri, DHS hizmeti veren kuruluşlar ve TÜBİTAK’ın sorumlulukları anlatılmaktadır.

Bu Kılavuzun III. Bölümünde, TSM’sini kendi kurmak ya da bir DHS’den temin etmek isteyen ÖKC Üreticilerinin başvuru süreçleri ve iş akışları tarif edilmektedir.

Bu Kılavuzun IV. Bölümünde, ÖKC TSM’lerinde gerçekleştirilecek onay denetimi ve periyodik bilgi sistem denetim faaliyetlerine ilişkin detaylar yer almakta, iş akışları ve denetim faaliyeti sonucunda düzenlenen raporların formatları düzenlenmektedir.

Bu Kılavuz ÖKC Üreticileri, ÖKC TSM hizmeti verecek kuruluşlar (ÖKC Üreticisi, ÖKC TSM veya ÖKC TSM hizmeti ile ilgili tüm Dış Hizmet Sağlayıcıları) ve ÖKC TSM Denetçileri için bağlayıcıdır.

BÖLÜM I

YENİ NESİL AKARYAKIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM GÜVENLİK GEREKSİNİMLERİ

2. Kritik Varlıklar ve Aktörler

Sistemde var olan ve ifşa olması veya değişikliğe uğraması durumunda sistemin gizliliğini, bütünlüğünü, kaynak/kimlik doğruluğunu ve erişilebilirliğini olumsuz yönde etkileyecek varlıklar aşağıda listelenmiştir. İlerleyen bölümlerde belirtilen gereksinimlere uyulmazsa aşağıda listelenen varlıkların biri veya birkaçı ifşa olabilir, bütünlüğü bozulabilir veya kullanılamaz/erişilemez duruma gelebilir.

2.1 Kritik Varlıklar

2.1.1 Birincil Varlıklar

Birincil varlıklar ÖKC TSM'sinden yönlendirilirken ya da ÖKC TSM'sinde bulunurken Bilgi İşlem Merkezi (BİM)'nin korumasını istediği varlıklardır.

2.1.1.1 YN Pompa ÖKC Plaka Bazlı Günlük Satış Raporu

Plaka bazlı günlük satış raporu, YN Pompa ÖKC'den BİM'e GMP dokümanında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmelidir.

ÖKC TSM bu varlık için yönlendirme işlemini yürütecektir.

2.1.1.2 YN Pompa ÖKC Anlık Fiş Bilgisi

YN Pompa ÖKC anlık fiş bilgisi, YN Pompa ÖKC'den BİM'e GMP dokümanında tanımlandığı gibi gizliliği ve bütünlüğü korunacak şekilde gönderilmelidir.

ÖKC TSM bu varlık için yönlendirme işlemini yürütecektir.

2.1.1.3 YN Pompa ÖKC Mali Uygulama Yazılımı

YN Pompa ÖKC mali uygulama yazılımı, ÖKC TSM tarafından güncellenecektir. YN Pompa ÖKC mali uygulama yazılımının inkâr edilemezliği TÜBİTAK OKTEM Laboratuvarının YN Pompa ÖKC yazılımının özetine uyguladığı imza veya Üretici imzası ile sağlanmaktadır.

ÖKC TSM bu varlığı açık olarak görebilmektedir.

2.1.2 İkincil Varlıklar

İkincil varlıklar, birincil varlıkları korumak için ÖKC TSM'sinin kullandığı aşağıda listelenen varlıklardır.

- Kriptografik anahtarlar
- ÖKC TSM sistem bileşenleri erişim denetim verisi (ÖKC TSM bileşenlerine yetkili kullanıcıların erişim izleri)
 - Sunucular
 - HSM cihazları
 - ÖKC TSM olay kayıtları (ÖKC TSM iz kayıtları)
 - Yazılımlar (ÖKC TSM'de kullanılan yazılımlar)

2.2 Aktörler

2.2.1 Yetkili Kullanıcılar

Yetkili kullanıcılar, sistemin tüm alt bileşenlerinde yer alan yetkilendirilmiş (kullanıcı adı /parola veya akıllı kartı olan) kullanıcılardır. Bu kullanıcılar, sadece normal veri akış senaryosunda yer alan kullanıcılarla sınırlı değildir. Kurulumcu, bakım/onarımcı, denetçi gibi farklı kullanıcılar da potansiyel tehdit kaynağı olarak görülmelidir.

Kullanıcılar farklı motivasyonlarla tehdit unsuru olabilir. Yetersiz eğitilmiş, hoşnutsuz, ihmalcı, kötü amaçlı, sahtekâr, işine son verilmiş veya işinden ayrılmış olabilirler. Bu kişiler; şantaj yapmak, özel bilgilere erişmek, bilgisayarları bozmak, sahtekârlık ve hırsızlık yapmak, bilgi rüşvetçiliği yapmak, tahrif edilmiş ve bozulmuş ya da yanlış veri girişi yapmak, kötü amaçlı kod (virüs, truva atı, vb.) yüklemek, kişisel bilgileri satmak, sistemi sabote etmek, kurum itibarını zedelemek veya yetki yükseltmek gibi çeşitli vesilelerle tehdit oluşturabilirler.

2.2.2 Yetkisiz Kullanıcılar (Hacker, Siber Terörist, vb.)

Yetkisiz kullanıcılar, sisteme herhangi bir atak yüzeyinden (örn: cihazlar, ağ üzeri) saldıran, genellikle sistem tarafından yetki verilmemiş kişi veya organizasyonlardır. Sistemi alt etme teşebbüslerinde farklı motivasyonlar olabilir: maddi kazanç, şöhret, otoriteye karşı verilen mücadeleden keyif alma, farklı bir ülke çıkarlarını koruma, operatörlere ve vatandaşlara yönelik sosyal mühendislik saldırıları, sistem açıklıkları, kriptografik saldırılar, yan kanal saldırıları, üretim sırasında müdahale gibi birçok tekniği kullanabilirler.

2.2.3 Teçhizat ve Yazılımlar

Ağ ve veri tabanı sunucusuna bağlanılmasını sağlayan teçhizat ve yazılımlar (bilgisayar, işletim sistemleri vb.) arızalandıklarında, kusurları olduğunda ya da güncel tutulmadıklarında çeşitli saldırılara maruz kalabilirler.

Teçhizat ve yazılımlar sahaya ilk çıktıklarında saldırmaya elverişli açıklık barındırabilirler. Bir diğer tehlike, teçhizat ve yazılımların sahada kullanıma çıktıklarında veya güncelleme, bakım/onarım aşamalarında saldırganlar tarafından kötücül yazılım (malware, trojan vb.) araçları vasıtasıyla saldırı amaçlı kullanılmalarıdır. Dolayısıyla, teçhizat ve yazılımlar bilgi kaçağı, yetkisiz erişim ya da hizmet engellemesine neden olabilirler.

2.2.4 Çevresel Koşullar

Bulunulan konum sebebiyle nem, ısı, ışık, sıcaklık vb. hava şartlarından kaynaklı olarak birçok farklılık olacaktır. Ortam sıcaklığının değişmesi nedeniyle, güvenlik fonksiyonlarının aksaması, cihazlardan bilgi kaybı, cihazın bozulmasıyla sistemin aksaması vb. durumlar meydana gelebilir.

3. Sistem Güvenliği, İş Sürekliliği, Felaket Kurtarma ve Olay Müdahale

✓ ÖKC TSM'sinin akredite kuruluşlardan alınmış ISO/IEC 27001 [1] sertifikasının bulunduğu görülmelidir. Sertifikanın Bölüm 2'de belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsadığı kontrol edilmelidir.

✓ ÖKC TSM'sinin akredite kuruluşlardan alınmış ISO/IEC 22301 [2] sertifikasının bulunduğu görülmelidir.

4. Kullanılan Donanımların Güvenliği

ÖKC TSM'lerinin; BİM ve YN Pompa ÖKC ile haberleşmek için kriptografik anahtarlar kullanması ve bu anahtarların ÖKC TSM'lerinde ISO/IEC 19790, Common Criteria EAL4+ veya FIPS 140-2 Level 3 ve üzeri için sertifika almış ürünler ile saklanması gerekmektedir.

5. Kullanılan Yazılımların Güvenliği

Yapılacak test ve değerlendirmeler sonucunda ÖKC TSM'sinin aşağıdaki görevleri yerine getirdiği anlaşılan yazılımlarının, PCI DSS denetim kapsamında olduğu görülmelidir.

Yazılımın güvenlik ile ilgili görevleri;

- YN Pompa ÖKC ile haberleşmeyi sağlamak
 - YN Pompa ÖKC 'lere mali uygulama yazılımını yüklemek
 - YN Pompa ÖKC 'lere mali parametreleri yüklemek
- BİM ile haberleşmeyi sağlamak
- YN Pompa ÖKC ile BİM'in haberleşmesini sağlamak
 - Mali bilgilerin gönderilmesi
 - Olay kayıtlarının gönderilmesi
- YN Pompa ÖKC'den olay kayıtlarının alınması

6. Güvenlik Denetimi

ÖKC TSM'lerinin aşağıda listelenen kapsamda Sızma Testi Raporunun bulunduğu ve her yıl yenilendiği görülmelidir. Sızma testinin Bölüm 2'deki tüm kritik varlıkları ve sistemin genelini kapsayacak şekilde yapıldığı kontrol edilmelidir. Sızma testinde açıklık tespit edilmişse, tespit edilen açıklığın giderilmesine yönelik müdahale planının olduğu bir rapor hazırlanmalıdır.

- ✓ Sosyal Mühendislik Testleri
- ✓ Ağ ve İletişim Altyapısı Testleri
- ✓ İşletim Sistemi ve Platform Testleri
- ✓ Uygulama Testleri
- ✓ Veri Tabanı Testleri

BÖLÜM II

YENİ NESİL AKARKAYIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM SİSTEM GEREKSİNİMLERİ

7. ÖKC TSM'lerinin Desteklemesi Gereken Standartlar

ÖKC TSM'lerinin aşağıdaki sertifikasyonlar için denetlemelerden geçmiş ve bu sertifikaları almaya hak kazanmış olmaları gerekmektedir. Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelikte açıklandığı şekilde ÖKC TSM'nin yılda bir kez denetlenmesi ve denetim mektubu ile güncellenmiş sertifikaların üye iş yeri anlaşması yapan kuruluşlara gönderilmesi gerekmektedir.

İlki başvuru sürecinde olmak üzere, üç yılda bir kez, ÖKC TSM'sinin bağımsız denetim kuruluşları tarafından gerçekleştirilecek Bilgi Sistemleri Denetimi ile proje genelinde hedeflenen bilgi güvenliği standardına ulaşıp ulaşılmadığı sınanmış olmalıdır. Tespit edilen açıklıkların kapatılmasına yönelik ÖKC TSM tarafından alınan aksiyonlar kontrol edilmelidir.

7.1 Uluslararası Standartlar

Uluslararası bilgi sistemleri ve ödeme sistemlerine ait aşağıdaki temel standartlar sağlanmalıdır. Bu standartların sağlandığı alınan sertifikalarla ispatlanmalıdır. Sertifikalar düzenli olarak yenilenmelidir. Sertifikalar ile ilgili detaylı bilgiye “**Referanslar**” bölümünde yer alan linklerden ulaşılabilmelidir.

a. PCI-DSS Payment Card Industry Data Security Standard Onay Belgesi

AOC (Attestation of Compliance for Onsite Assessments) Belgesi üzerinde ÖKC TSM hizmetlerinin verildiği uygulamaların denetim kapsamında olduğunun, sertifikanın Bölüm 2'de belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsadığının kontrol edilmesi gerekmektedir.

Sertifikasyon asgari olarak *Infrastructure/Network, Payment Gateway/Switch, Backoffice Services ve POS/Card Present* için alınmış olmalıdır. AOC (Attestation of Compliance for Onsite Assessments) dokümanında bu başlıklardan onay alındığı görülmelidir.

Ayrıca AOC içerisinde *Other Processing (specify)* alanında "*Trusted Service Manager Services*" ibaresi bulunmalıdır veya *Description* alanında ÖKC TSM hizmetlerinin kapsamda olduğu ifade edilmiş olmalıdır.

YN Pompa ÖKC'ler, ÖKC TSM ve üye işyeri anlaşması yapmış kurumlar arasındaki iletişim güvenliği için PCI DSS onaylı bir anahtar yönetim mekanizması kurulmuş olmalıdır.

- b. ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi
- c. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi
- ç. ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi

7.2 Ulusal Standartlar

Ulusal ödeme sistemleri kural koyucuları ve mali kural koyucular (Başkanlık) tarafından belirlenen ve güncellenen standartlara uyulması gerekmektedir.

8. ÖKC TSM Başvuru, Test, Denetim ve Onay Süreçleri

ÖKC TSM'lerinin başvuru, test, denetim ve onay süreçleri Bölüm III'te detaylı olarak anlatılmaktadır. ÖKC TSM'lerinde ÖKC Üreticileri için münhasıran kurulmuş bir donanım, yazılım ve işletim sistemi olup olmadığı incelenecek ve sertifikalar bu sistem için alınmış olacaktır.

9. Sistemlerin Münhasırlığı

✓ ÖKC TSM altyapısı için kullanılan uygulama sunucuları her ÖKC Üreticisi için ayrı bir fiziki ve/veya sanal ortamda kurulabilir. Kurulan bu fiziki ve/veya sanal ortamlar sadece YN Pompa ÖKC altyapısına hizmet veren sanal ve/veya fiziksel sunucuların üzerindeki görevler (Servisler, uygulamalar vb.) PCI-DSS kriterlerine uygun şekilde yapılandırılmalıdır.

✓ ÖKC TSM altyapısında kullanılan veri tabanı sunucuları her ÖKC Üreticisi için ayrı bir fiziksel ve/veya sanal sunucuda kurulmalıdır. Veri tabanı sunucularına ait veriler her Üretici için kendisine ait disk gruplarında barındırılmalıdır.

✓ Sanallaştırma sistemlerine ait fiziksel sunucular (Vmware, Hyper-V vb.) üzerinde ÖKC TSM sistemleri dışında sanal sunucular varsa, ÖKC TSM sistemleri diğer sunuculardan ağ bazında tamamen izole olarak ayrı sanal lokal ağlarda (VLAN) kurulmalıdır. ÖKC TSM sistemleri

kendi içinde de PCI-DSS kriterlerine uygun olarak rol bazında da (Web sunucu, uygulama sunucu, veri tabanı sunucusu gibi) ayrı sanal lokal ağlarda (VLAN) izole edilmelidir.

✓ ÖKC TSM ve ikincil merkezde bulunan ağlar, ÖKC TSM sistemlerini varsa diğer tüm sistemlerden izole edecek şekilde (Sanal lokal ağlar kullanılarak) yapılandırılmalıdır. ÖKC TSM omurgasında ortak olarak kullanılan tüm cihazlar (Firewall, Load Balancer, Switch, Storage, vs) üzerindeki konfigürasyonlar mantıksal seviyede izole edilerek hazırlanmalıdır.

✓ Veri tabanı sunucuları ayrı bir ağ altında bulunmalı ve sanal lokal ağlarla (VLAN) diğer uygulamalardan ayrılmalıdır. Bu VLAN'lara erişim sadece kontrolsüz ağlara erişimi olmayan uygulama sunucularından ve en az mantıksal seviyede sağlanmalıdır.

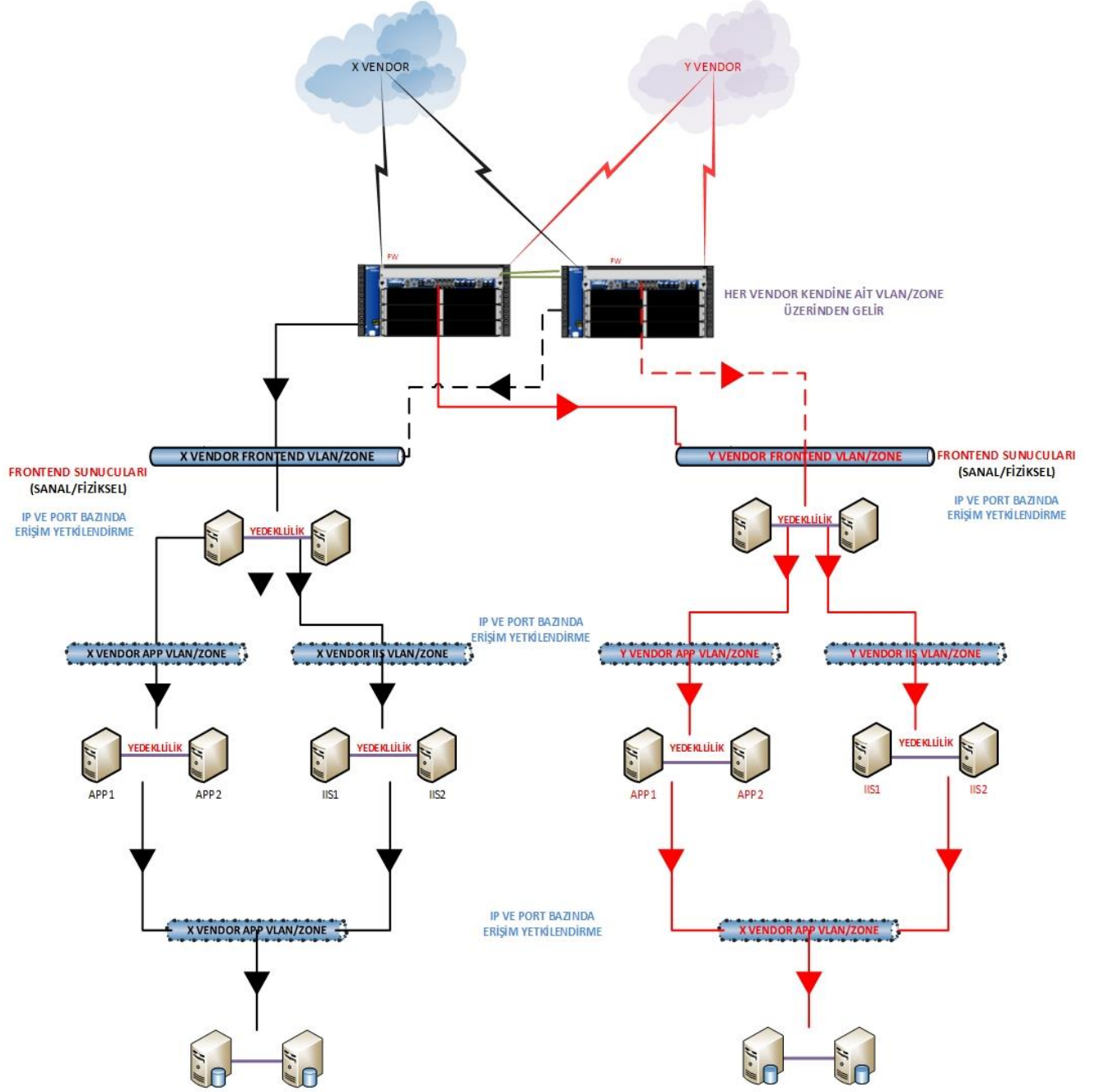
✓ HSM cihazları ve sunucuları farklı ÖKC Üreticileri için farklı kriptografik anahtarlar kullanılmak şartıyla ortak olarak kullanılabilir.

✓ Tüm sistemlerde erişim yetkileri PCI-DSS standartlarına göre belirlenmeli, uygulanmalı ve belgelendirilmelidir. Ayrıca PCI-DSS standartları gereği yıllık olarak BDK tarafından denetlenmelidir.

✓ Yukarıda bahsedilen münhasırlık maddeleri ÖKC TSM'lerinin ikincil merkezleri için de geçerlidir.

Birden fazla ÖKC Üreticisine hizmet veren örnek bir ÖKC TSM'sinin sistemlerinin münhasırlığına ilişkin topoloji aşağıdaki şekilde gösterilmektedir. Bu şekil, münhasırlık prensiplerinin uygulanabileceği örnek bir şekil olup, uygulanması zorunlu değildir.

ÖRNEK DHS TSM TOPOLOJİSİ



1. Her üreticiye ait terminaler, gerekli izolasyon sağlanmış (APN, Ip tanımı, Tunnel vs) çeşitli bağlantı yöntemleri ile TSM güvenlik duvarına gelir.
2. Güvenlik duvarları üzerinde her bir üretici için ayrı olarak tanımlanmış ZONE/ VLAN'lar gelen trafikleri karşılar ve sadece ilgili Frontend alanına gönderir.
3. Frontend alanında bulunan donanımlarda işleme tabi tutulan trafik, yine güvenlik duvarı üzerinden (L3 seviyesinde) kendisine ait Core Application ya da IIS makinalarına yönlendirilirler.
4. Core alanlarda bulunan donanımlar dışında veri tabanına hiç bir erişim bulunmamaktadır. Veri tabanlarına sadece Core alanlardaki sunucu/donanımlar erişebilir. Veritabanına yapılacak network erişimleri için trafik, güvenlik duvarı üzerinden (L3 seviyesinde) geçer.

10. ÖKC TSM'leri Sorumluluk Dağılımı

YN Pompa ÖKC'lerin yaşam döngüsü yönetimi ÖKC TSM üzerinden yapılacaktır. ÖKC TSM'sinin yönetim, yetki ve sorumluluğu ise ÖKC Üreticilerindedir. ÖKC Üreticilerinin bir DHS'den ÖKC TSM'sine ilişkin hizmet temin etmesi durumunda ÖKC Üreticisinin, ÖKC TSM hizmetlerine ilişkin sorumluluklarını ortadan kaldırmamaktadır. ÖKC Üreticileri ÖKC TSM'lerine ilişkin hizmetlerin sunumunda DHS'lerden de hizmet temin edebilir. Başkanlık açısından muhatap ÖKC Üreticisidir. ÖKC Üreticilerinin dış hizmet alımlarında riskini yönetebilmek adına DHS'lerle yaptığı anlaşmaları bu Kılavuzu dikkate alarak yönetmesi gerekmektedir.

ÖKC Üreticileri, kendi kuracakları ÖKC TSM'lerine ait birincil merkezinin donanım altyapısı ile tüm işletim ve operasyon süreçlerini dış kaynak kullanımı veya barındırma hizmeti şeklinde başka bir alt yükleniciden/taşerondan sağlayamaz. Birincil merkezin tüm işletim ve operasyon süreçlerini ÖKC Üreticisi 7/24 kendi personeli ile yürütmek zorundadır. İstihdam edilecek personelin nitelik ve niceliği ile ilgili "ÖKC TSM Personel Gereksinimleri" başlığında detaylı bilgi verilmektedir. Söz konusu donanım, tüm işletim ve operasyon süreçlerinin herhangi bir kısmının ÖKC Üreticisi dışında bir dış kaynaktan temin edilmesi halinde söz konusu ÖKC TSM DHS'nin verdiği bu hizmetler bakımından da test, değerlendirme, denetim ve onay süreçlerine tabi tutulacaktır.

ÖKC Üreticileri kendi kuracakları ÖKC TSM'lerine ait ikincil merkezinin; sadece donanım altyapısının barındırılması hizmetini taşeron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım altyapısının yönetimi ile tüm işletim ve operasyon süreçlerinin ÖKC Üreticisinin kendi personeli ile yürütmesi zorunludur.

YN Pompa ÖKC'ler üzerinde veya YN Pompa ÖKC'ler ile birlikte çalışacak cihazlar (EFT-POS, PinPad) yoluyla üye işyeri anlaşması yapan kuruluşun uygulamalarının çalıştırılmasına ilişkin sahada yapılması gereken tüm servis ve saha operasyonlarının yetki ve sorumluluğu ÖKC Üreticilerindedir.

ÖKC TSM ve DHS'ler vereceği hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırmak zorundadır.

11. Mükellef, YN Pompa ÖKC, ÖKC TSM'leri ve BİM İletişimi

YN Pompa ÖKC'ler, BİM'e ÖKC TSM'leri üzerinden bağlanacak olup, cihazların doğrudan veya ÖKC TSM'leri haricinde başka bir hat üzerinden BİM'e bağlanması mümkün değildir. ÖKC TSM'leri ile YN Pompa ÖKC'ler ve BİM arasındaki kurulacak olan güvenli altyapı, ağların sorumluluğu ve sahipliği (tasarrufu) ÖKC Üreticilerinde olacaktır. YN Pompa ÖKC'lerin ÖKC TSM'lerine erişimleri için gereken altyapı, erişim hatlarının sorumluluğu ve sahipliği ise YN Pompa ÖKC kullanan mükelleflere aittir.

YN Pompa ÖKC'lerin ÖKC TSM'leri üzerinden BİM'e gönderecekleri mesajların sadece BİM tarafından kayıt ve analiz edilebilecek mahiyette olması ve ilgili mesajlaşma protokollerine uygun şekilde gönderilmesi esastır.

ÖKC TSM'leri ve DHS'lerin, EFT-POS özellikli YN Pompa ÖKC'ler ve haricen EFT-POS ile entegre çalışan YN Pompa ÖKC'ler de dahil, üzerinden bankacılık mesajlarının da geçecek olması nedeniyle BDDK ve PCI SSC'nin gerektirdiği düzenleme ve standartları karşılaması zorunludur.

Üye işyeri anlaşması yapan kuruluşlara ait olanlar da dahil olmak üzere YN Pompa ÖKC'ler üzerinde çalışan tüm uygulamalar ÖKC TSM üzerinden banka ya da diğer uygulama sistemlerine bağlanacaktır. (ERP programlarına GMP3 ile kablolu bağlanılabilir). Üye işyeri anlaşması yapan kuruluşun yetkilendireceği kişi ve/veya kurumlar, YN Pompa ÖKC ile birlikte çalışacak bankacılık uygulamaları ve bunlara ilişkin parametre, anahtar yazılım yükleme ve ihtiyaç duyulan diğer işlemleri yerine getirmek için taleplerini ÖKC TSM'lerine bildireceklerdir. Bu işlemler ÖKC TSM'leri aracılığıyla gerçekleştirilecektir. YN Pompa ÖKC'ler parametre veya yazılımları ÖKC TSM üzerinden geçmek kaydıyla doğrudan talep ederek de alabilirler. YN Pompa ÖKC parametre yönetiminde, cihazın genel işlevine etki eden parametreler (cihazın açılması, kapanması, işlevsel olarak devre dışı kalması gibi diğer uygulamaların çalışmasını etkileyecek genel cihaz parametreleri) sadece ÖKC TSM'leri tarafından yönetilmeli, diğer uygulamalara bırakılmamalıdır. YN Pompa ÖKC, ÖKC TSM'leri ve üye işyeri anlaşması yapmış kurumlar arasındaki güvenli iletişim için kullanılacak anahtarların yönetim mekanizmaları PCI DSS'nin kabul ettiği mekanizmalar olmalıdır. YN Pompa ÖKC'lerde oluşabilecek sorunlardan (sahada yaşanacak cihaz ya da tüm uygulamalardaki manipülasyonlar, alınan ödeme ile kesilen mali fiş mutabakatsızlıkları, fonksiyonel arızalar, usulsüz banka/sadakat uygulama anahtar yüklemeleri, saha operasyonel sıkıntıları vb.) ÖKC Üreticileri sorumludur.

ÖKC TSM, Başkanlık ve yasalarca yetkili kılınmış diğer kurumlardan gelen talimatlar doğrultusunda YN Pompa ÖKC'lerin fonksiyonlarının tümünü veya belli bir kısmını uygun denetim izleri bırakarak tamamen ya da geçici süreyle durdurabilir veya değiştirebilir.

Üye işyeri anlaşması yapan kuruluşlara ait kural koyucular tarafından hassas veri olarak kabul edilen veriler ÖKC TSM üzerinden iletilirken hiç bir durumda (Banka ve kurumlara kredi kartı, banka kartı, POS, sanal POS, elektronik ticaret, ATM işletimi vb. ödeme sistemleri hizmetleri verilmesi hariç) açılmamalı veya saklanmamalıdır. ÖKC TSM'lerinin, müşteriler (kart hamilleri) ile ilişkilendirilebilecek hiçbir veriye ve kural koyucular tarafından hassas veri olarak tanımlanan verilere erişebilme kabiliyeti bulunamaz.

12. YN Pompa ÖKC Mesajlarının Yönetimi

YN Pompa ÖKC mesajları, ÖKC TSM üzerinden BİM'e GMP'ye uygun olarak iletilir.

YN Pompa ÖKC'ler GMP dokümanına uygun olarak, sadece ÖKC TSM'lerine bağlı olarak çalışmak ve ÖKC TSM'leri üzerinden BİM ve üye işyeri anlaşması yapan kuruluşlar ile haberleşmek zorundadırlar.

13. Risk Yönetimi Esasları

ÖKC TSM'si bilgi teknolojilerindeki riskler, kurumdaki tüm risklerin bir parçası olarak belirlenmeli, ölçülmeli ve yönetmelidir. Risk yönetim çerçevesi, bilgi teknolojilerindeki genel risk seviyelerini, risk oluştuğunda karşılama stratejilerini belirlemelidir. Bu amaçla bir "Risk Komitesi" oluşturulmalıdır.

Mevcut yapının hedefleri üzerinde herhangi bir potansiyel etkinin oluşturacağı beklenmedik durumlar önceden tespit edilmeye çalışılmalıdır. Artakalan riskleri kabul edilebilir bir seviyeye ulaştırmak için risk karşılama stratejileri uygulanmalıdır. Risk analizi sonrası riskler tanımlanmalı, sınıflandırılmalı ve derecelendirilmelidir. Tanımlama, sınıflandırma ve derecelendirme sonrasında sonuç raporlanmalıdır. Tanımlanan riskler önceliklendirilmeli ve uygun risk karşılama stratejisi belirlenmelidir.

Önemli değişikliklerden önce risk analizi yapılmalı ve analizlere ilişkin yazılı politikalar belirlenmelidir. Yapılan değişiklik sonrası durum raporlanmalıdır.

Risk analizi belirlenmesi, analiz edilmesi ve izlenebilmesi için risk yönetim politikaları belirlenmeli ve politikaların destekleneceği dokümanlar oluşturulmalıdır. Riskleri yönetebilmek için önceliklerin ve risklerin neler olduğunun bilinmesi gerekmektedir. Bu sebeple, önem dereceleri ve riskler gerçekleştiğinde oluşan etkiler göz önüne alınarak, kabul edilebilir risk toleransı ve bu duruma uygun kontroller tanımlanmalıdır. Roller ve sorumlulukların tanımlanması ile rehberlik ve talimatların sağlanması için politika, prosedür, kılavuzlar ve standartlar geliştirilmelidir. Bunlar yılda en az bir kez kontrol edilerek güncellenmelidir. ÖKC TSM kendi iş süreçlerini oluşturan teknik raporu ÖKC TSM onay başvurusu sırasında teslim etmelidir.

Erişim, kimlik doğrulama, yetkilendirme kontrolü belli aralıklarla kontrol edilmeli ve tekrarlanmalıdır. Sistemlere erişimler kayıt altında tutulmalı ve farklı bir ortamda saklanmalıdır.

14. Değişiklik Yönetimi

ÖKC TSM, bünyesindeki bilgi sistemleri üzerinde gerçekleştirilen ve YN Pompa ÖKC mesajlarını yöneten donanım ve yazılımlara ilişkin her türlü bakım, yama ve değişikliğin uygun bir şekilde planlanmasını, yetkilendirilmesini, test edilmesini, gerçekleştirilmesini, belgelendirilmesini ve sonrasında denetlenebilirliğini sağlayacak yazılı ve etkin bir değişiklik yönetimi süreci işletmelidir.

ÖKC TSM, YN Pompa ÖKC mesajını yöneten yazılımlar için, yazılım geliştirilen ortamların ve geliştirilen yazılımların canlı ortama aktarılmadan önce test edildiği ortamların canlı ortamlardan ayrılmasını ve bu ortamların herhangi birinde değişiklik yapma yetkisine sahip personelin diğerlerinde değişiklik yapma yetkisinin bulunmamasını sağlar. Test ve geliştirme ortamlarında kullanılan verilerin canlı ortam verileri ile eşleştirilemez nitelikte olmasını temin eder.

ÖKC TSM, YN Pompa ÖKC mesajını yöneten sistemlere ilişkin değişikliklerde etki analizi yapılmasını, değişikliğin yetkili kişi veya kişilerce onaylanmasını ve değişikliği geri çekme prosedürünün oluşturulmasını sağlar.

15. Denetim İzlerinin Oluşturulması

ÖKC TSM'leri, ÖKC mesajlarının yönetildiği sistemlere ve yazılımlara gerçekleştirilen mantıksal veya fiziksel erişimlere, işlem altyapısını kullanan yetkisiz erişim teşebbüslerine ilişkin etkin bir denetim izi mekanizması tesis eder.

Denetim izi, kullanıcılara sorumluluk atayan, yeterli detay içeren ve şüpheli bir olayı izleme imkânı sunan nitelikte tutulur.

Denetim izleri asgari olarak aşağıdaki bilgileri içerir.

- İşlemi gerçekleştiren uygulama ve/veya işlemi gerçekleştiren ve varsa onaylayan kişiler,
- İşlemin açıklaması,
- Yapılan işlemin zaman bilgisi,
- İşlemin olumlu veya olumsuz sonucu,
- Etkilenen veri ve sistemlerin bilgisi.

YN Pompa ÖKC'lere ÖKC denetim izi oluşturulmadan bir yazılım veya parametre yükleme emri oluşturulamaz. Bu emrin oluşturulması için emrin sisteme kaydedildiği ilk andan itibaren tüm aşamaların iz kaydı oluşturulur ve saklanır. Söz konusu emrin bir dış sistem tarafından alındığı durumda, bu emrin hangi dış sistem tarafından ne zaman ve ne şekilde alındığı sorgulanabilmeli ve görüntülenebilmelidir.

ÖKC TSM'sinde bulunan sistemlere erişimlerin, denetim izlerinin prosedürlerde belirtilen sistemler için, prosedürlerde belirtildiği şekilde tutulduğu ve düzenli olarak gözden geçirme ve izlemeye tabi tutulduğu incelenmelidir. Denetim izi olarak hangi parametrelerin (örneğin başarılı ya da başarısız giriş denemeleri, bilgi sistemleri üzerinde yapılan faaliyetler vb.) tutulacağına ilişkin belirlemenin yapılacağı kontrol edilmelidir.

ÖKC TSM bünyesinde, kullanıcıların bilgi kaynaklarına erişimleri ile ilgili denetim izlerinin tutulmasına dair bir politika ya da prosedürün olması gerekmektedir.

YN Pompa ÖKC sisteminin altyapısına ait sistem/güvenlik izleme araçlarının kullanıldığı ve bu araçlar tarafından üretilen kayıtların tutulduğu ve takip edildiği gözlemlenmelidir.

Yedeklemelere ilişkin denetim izleri yedekleme periyodlarına uygun bir aralıkta log tutulmalı ve bu logların geçerliliği kontrol edilmelidir.

ÖKC TSM'sinde bulunan sistemler üzerinde, sistem ve kullanıcı işlemlerinin denetim izlerinin ne şekilde ve nasıl saklandığı öğrenilmeli ve ilgili personel tarafından düzenli olarak gözden geçirildiğine ilişkin kanıtlar temin edilerek incelenmelidir.

Denetim izleri asgari 5 yıl süreyle denetime hazır bulundurulacak şekilde ÖKC TSM'leri tarafından saklanır.

Denetim izlerinin bütünlüğünün sağlanması ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır.

Denetim izlerinin güvenli ortamlarda saklanması gerekmektedir.

ÖKC Üreticisi, denetim izlerinin düzenli olarak gözden geçirilmesine, değerlendirilmesine ve raporlanmasına ilişkin iç süreçlerini oluşturur.

Denetim izi oluştururken ÖKC mesajlarının ve ödeme sistemi hassas verilerinden herhangi birinin tamamının (örneğin kart numarasının tamamının yazılmaması gibi) kullanılmaması esastır.

16. Anahtar Yönetim Süreçleri ve Veri Güvenliği

YN Pompa ÖKC ile ÖKC TSM arasındaki tüm mesajlar ilgili teknik kılavuzlara uygun olarak GMP dokümanında belirtildiği şekilde şifrelenmelidir.

YN Pompa ÖKC ile ÖKC TSM arasındaki tüm anahtar yönetim mesajlarında kimlik doğrulama, veri bütünlüğünü sağlama, gizlilik ve mahremiyeti temin etme ve inkâr edememe şartlarını sağlama amaçlarıyla kullanılabilen, literatürde kabul görmüş ve güvenilirliğini yitirmemiş güçlü bir algoritma kullanılmalıdır.

Tüm kriptolojik anahtarlar, güvenliği uluslararası standartlarca belirlenmiş şifreleme donanımlarında veya bu anahtarları saklayabilecek, şifreleyebilme seviyesine sahip olduğu bilinen algoritma ve anahtarların kullanımı ile güvenli saklama ortamlarında korunmalıdır. Söz konusu anahtar şifreleme anahtarları, mutlaka güvenliği uluslararası standartlarca belirlenmiş şifreleme donanımlarında saklanmalıdır.

17. Yazılım Güvenliđi ve Sorumluluđu

ÖKC TSM'sinde çalışan yazılımların güvenliđinden ÖKC TSM'si, ÖKC Üreticisine karşı sorumludur.

Yazılım geliştirme esnasında tüm geliştirme süreçlerinin ve tarihçesinin gözlemlenebildiđi ve tüm geliştirici adımlarının takip edilebildiđi denetlenebilir kaynak kod kontrol/sürüm yönetim sistemleri kullanılmalıdır.

Geliştirilmiş olan yazılımın tüm tarihçesi ve hangi geliřtirmenin kim tarafından hangi sürüm için yapılmış olduđu bu sistemler tarafından izlenebilir olmalıdır.

YN Pompa ÖKC'ler üzerine yüklenecek olan tüm uygulamaların kaynađının dođrulanması sağlanmalıdır. Sadece kaynađı dođrulanmış ve güvenilir kaynaklardan gelen uygulamalar yüklenmelidir.

ÖKC TSM'leri aracılığıyla YN Pompa ÖKC'lere yüklenecek yazılımlara ilişkin sürüm, tarih ve açıklama bilgilerinin ÖKC TSM'sine bildirilmesi ve ÖKC TSM'leri tarafından kontrol edilerek kaydedilmesi gerekir.

18. İş Sürekliliđi Yönetimi

ÖKC TSM, iş süreklilik ve acil durum prosedürlerini hazırlamış ve işletiyor olmalıdır.

ÖKC TSM, iş sürekliliđi standartlarına uygun olacak şekilde bilgi sistemleri servislerinin, aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek sistem mimarisini tasarlamış ve işletiyor olmalıdır.

Kullanılan uygulamalar birbirlerini yedekleyecek şekilde kurulmuş sunucular üzerinde yedekli olarak barındırılmalı ve yayımlanmalıdır.

Yılda 4 defa tüm sistemlere ait iş sürekliliđi iç testleri gerçekleştirilerek kayıt altına alınmalıdır. Testlerden ortaya çıkan tüm sonuçlar risk yönetimi prosedürlerine ya da iş sürekliliđi eğitimlerine dahil edilmelidir.

ÖKC TSM, iş sürekliliği planlamasına yönelik olarak iş etki analizi yapmalı ve kurtarma stratejilerini belirlemelidir. Bu kapsamda, iç ve dış bağımlılıklar belirlenmeli ve meydana gelebilecek bir kesinti durumunda gereken faaliyet düzeyini ortaya koymak üzere operasyonlar önem düzeyi açısından sınıflandırılmalıdır. Farklı kesinti senaryolarının faaliyetler üzerinde yaratabileceği muhtemel riskler ve bunların potansiyel etkileri ÖKC TSM'si tarafından değerlendirilmelidir.

İş Sürekliliği Dokümanında, belirlenmiş süreçlerde sürekliliği etkileyebilecek durumlar oluşmadan, oluşma sırasında ve sonrasında kullanılacak yöntemler belirlenmeli ve belgelendirilmelidir.

Süreç kapsamında sistemlerin performans takibi ve uyarı mekanizmaları için bir alt sistem ya da uygulama kullanılmalıdır. Bu ürün ile sunucular, işletim sistemleri, işletim sistemi servisleri, veri hatları, network aktif cihazları vb. sistem bileşenleri, her cihaza özel parametreler ve eşik değerleri kullanılarak 7/24 esasına göre işletim ekipleri tarafından izlenmelidir. Aynı zamanda bu uygulama aracılığıyla, sistem bileşenlerinin belirlenmiş herhangi bir eşik değerinin aşılması durumunda sisteme tanımlanmış personele uyarı mesajlarını SMS ve/veya e-mail yolu ile gönderilerek gerektiğinde yine önceden belirlenmiş otomatik prosedürler ile müdahale edilmelidir.

İletişim kanalları ve veri hatları yedekli olarak çalışmalı ve sonlandırılmalıdır.

ÖKC TSM'si felaket durumunda sistemin çalışırılığını sağlayabilmek için aşağıdaki şartları sağlayan bir ikincil merkez oluşturmalıdır;

- İkincil merkez, ÖKC TSM'sinden coğrafi olarak aynı riskleri taşımayan en az 300 km uzaklıkta bir lokasyonda kurulmalıdır.
- İkincil merkezde tüm elektrik ve soğutma sistemleri yedekli olarak bulunmalı, ayrıca yangın, su baskını, sel vb. doğal afetlerden de korunma sağlanmalıdır.
- İkincil merkezde kurulan altyapı ÖKC TSM'sine gelen işlem kapasitesini karşılayacak seviyede olmalıdır.
- İkincil merkez felaket durumunda en geç 60 dakika içinde, en fazla 30 dakikalık veri kaybı ile ayağa kaldırılabilir.
- Birincil merkezin olağanüstü bir durum nedeniyle hizmet veremez duruma gelmesi halinde ikincil merkeze geçilmesine yönelik acil durum planı yapılmalı, plan 6 aylık

periyodlar ile kontrol edilmeli ve gerektiğinde güncellenmelidir. İkincil sistemin çalışırılığı yıllık olarak test edilmeli ve yıllık testler raporlanmalıdır.

Acil Durum Planı hazırlanırken;

- Kimin, nereye, nasıl müdahale edeceğini belirleyen prosedürler ve süreçler tanımlanmalıdır. Bu prosedür ve süreçler, sistemi izleyen işletim personelinin elektronik ve basılı ortamda kolayca ulaşabileceği şekilde bulundurulmalıdır.
- Beklenmedik olay meydana geldiğinde “ilk tespit, tespitin sorumlusuna atanması, kesin tespit, çözüm önerisi ve çözüm aksiyonunun alınması” yetkileri belirlenmiş ve belgelendirilmiş personellere atanmalı ve aksiyonlar takip edilerek raporlanmalıdır.

ÖKC TSM sistem odası asgari olarak aşağıdaki kriterlerde Uptime Institue Tier 2 standartlarında belirtilen kriterlere uyumlu olacaktır.

- Yedekli Klima – İklimlendirme
- Yedekli Kesintisiz Güç Kaynağı (2 UPS)
- Sistem Odası Yedekli Jeneratör
- Yükseltilmiş Döşeme
- Sistem Operasyon Vardiya Düzeni
- Otomatik Yangın Söndürme Sistemi
- Sistem Odası Erişim Kontrolü
- Sistem Odası CCTV

ÖKC TSM’si tarafından plansız kesintiler olay inceleme raporu ile belgelendirilmiş olmalıdır.

ÖKC TSM’si, ÖKC TSM bilgi sistemleri servislerinin, aylık %99,75 kullanılabilirlik ile hizmet sunmasını temin edecek şekilde, mimari tasarımın ve testlerin yapıldığına dair güvence sunar. Kesinti süreleri yıllık plansız toplam 18 saati ve planlı bir defada 1,5 saati aşmayacak şekilde yılda 4 defadan (toplam 6 saatten) fazla olamaz. Planlı kesintilerin ÖKC TSM’sinden hizmet almakta olan üye işyeri anlaşması yapan kuruluşlara en az 5 gün önceden gerekçeleri ile birlikte bildirilmesi zorunlu olup planlı kesintilerin günün yoğun olmayan saatlerinde gerçekleştirilmesi

gerekmektedir. ÖKC TSM'si aylık olarak kullanılabilirlik raporunu hazırlayacak ve Başkanlığa ve ÖKC TSM hizmeti almakta olan üye işyeri anlaşması yapan kuruluşlara sunacaktır. Bu rapor aylık olarak denetimlerde sunulmak üzere hazır bulundurulacaktır. Kullanılabilirlik raporlarının incelenmesinde ve ÖKC TSM'lerinin kullanılabilirlik aylık oranının hesaplanmasında BİM kaynaklı ve ÖKC TSM'sine harici kaynaklardan gelen problemler tespit edilmiş olmalı ve ÖKC TSM'lerinin kullanılabilirlik değerlerine (oranlarına) negatif etkisi dikkate alınmamalıdır.

19. Dış Hizmet Alımı

ÖKC Üreticisi, ÖKC TSM hizmetini tamamen kendisi sağlayabileceği gibi, bu hizmetlere ilişkin DHS'den de hizmet alabilir. ÖKC Üreticileri, DHS'lerin bu dokümanda belirlenen temel koşullar ile uyumlu olduğuna ve sistem altyapısının güvenlik seviyesini düşürmediğine ilişkin, DHS nezdinde gerçekleştirdiği denetimlerle veya başka taraflarca gerçekleştirilen yerinde denetimler sonucunda oluşturulan onay belgelerinden faydalanarak emin olur. Ayrıca buna ilişkin belgelendirme dokümanlarını kendisinde muhafaza eder ve talep edilmesi halinde Başkanlığa sunar. ÖKC Üreticisi, ÖKC TSM'sine ilişkin DHS'den temin ettiği hizmetler için de asıl sorumlu olup, DHS'den temin edilen hizmetler de, hizmetin niteliğine bağlı olarak bu Kılavuzda belirlenen güvenlik ve sistem gereksinimlerine haiz olmalıdır.

ÖKC TSM'sine ilişkin DHS'den temin edilen ÖKC TSM hizmetlerinin, bu Kılavuzun 9 numaralı bölümünde yer alan “Sistemlerin Münhasırlığı” ilkesine uygun olarak verildiğinden emin olunmalıdır. ÖKC Üreticisi, ÖKC TSM hizmetini sunduğu sistemi yöneten ve 7/24 takip eden bir ekibin kendi sorumluluğu altında görevlendirilmesini sağlamalıdır.

ÖKC TSM'lerinin birincil ve ikincil sistemleri (DHS'den temin edilenler dahil) yurtiçinde olmak zorundadır. ÖKC TSM'lerine ilişkin ikincil sistemlerin; birincil sistemden farklı bir il sınırları içinde ve aralarında en az 300 km mesafe bulunacak şekilde kurulmuş olması zorunludur.

ÖKC Üreticileri, kendi kuracakları ÖKC TSM'lerine ait birincil merkezinin donanım altyapısı ile tüm işletim ve operasyon süreçlerini dış kaynak kullanımı veya barındırma hizmeti şeklinde başka bir alt yükleniciden/taşerondan sağlayamaz. Birincil merkezin tüm işletim ve operasyon süreçlerini ÖKC Üreticisi 7/24 kendi personeli ile yürütmek zorundadır. İstihdam edilecek personelin nitelik ve niceliği ile ilgili “ÖKC TSM Personel Gereksinimleri” başlığında detaylı bilgi verilmektedir. Söz konusu donanım, tüm işletim ve operasyon süreçlerinin herhangi bir kısmının ÖKC Üreticisi dışında bir dış kaynaktan temin edilmesi halinde söz konusu ÖKC

TSM'si DHS'nin verdiđi bu hizmetler bakımından da test, deęerlendirme, denetim ve onay süreçlerine tabi tutulacaktır.

ÖKC Üreticileri kendi kuracakları ÖKC TSM'lerine ait ikincil merkezinin; sadece donanım altyapısının barındırılması hizmetini taşıron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım altyapısının yönetimi ile tüm işletim ve operasyon süreçlerinin ÖKC Üreticinin kendi personeli ile yürütmesi zorunludur.

DHS, ÖKC TSM'lerine ait ikincil merkezinin; sadece donanım altyapısının barındırılması hizmetini taşıron ya da alt yükleniciden temin edebilir. Ancak, ikincil merkeze ait donanım altyapısının yönetimi ile tüm işletim ve operasyon süreçlerinin yönetiminin ilgili DHS/ÖKC Üreticisine ait personel tarafından yürütölmesi zorunludur.

20. Personel Gereksinimleri

ÖKC TSM'lerinde, Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Teknik Kılavuzu'nun ÖKC TSM tanımında belirtilen sistemlerin münhasırlığı prensibine göre ÖKC TSM'sinin yönetim ve sürekliliđi için ÖKC Üreticisine veya ÖKC Üreticisinin sorumluluđu altında DHS'ye ait yeterli düzeyde personel istihdam edilmelidir. İstihdam edilmesi tavsiye edilen personelin görevleri ve nitelikleri aşağıda belirtilmiştir.

Aşağıdaki rollerin her birini yapabilecek en az bir kiři görevlendirilmelidir. Aynı kiři birden fazla konuda görevlendirilebilir.

20.1 Network & Network Güvenlik Grubu:

(Grupta en az 3 kiři olmalıdır.)

- Network Uzmanı (Admin) & Mühendisi
- Network Güvenlik Mühendisi
- Bilgi Güvenliđi Uzmanı

20.2 Sistem ve Database Grubu:

(Grupta en az 3 kiři olmalıdır.)

Sistem, veri tabanı ve sistem operasyon birimlerinin prosedürlere uygun bir şekilde yönetimini sağlamaktadır.

- **Sistem Yöneticisi:** ÖKC TSM’inde bulunan ve sistemlerin/donanımların bakımı, işletilmesini sağlayan birimlerden sorumludur.
- **Sistem ve Sanallaştırma Mühendisi:** İşletim sistemleri, IIS, Exchange vb. Microsoft sistemlerinin kurulması, yönetilmesi ve sürekliliğinin sağlanması, Vmware, Hyper-V vb. sanallaştırma sistemlerinin kurulması, yönetilmesi ve sürekliliğinin sağlanmasından sorumlu olup bu sistemlere bağlı storage ve depolama ve donanım altyapılarına da bakmakla, işletmekle sorumludur.
- **Veri Tabanı Uzmanı:** MS SQL, Oracle, MySQL vb. veri tabanlarının kurulması, yönetilmesi, sürekliliğinin sağlanmasından sorumludur.

20.3 Sistem ve Terminal Operasyon Grubu:

(Grupta en az 10 kişi olmalıdır.)

- **Sistem Operasyon Yöneticisi:** Sistem operatörlerinden sorumlu olup, ÖKC TSM’inde yürütülen günlük operasyonel işlerin sürdürülmesinden ve takip edilmesinden sorumludur.
- **Sistem Operatörleri (Vardiyalı) :** ÖKC TSM’inde de kurulmuş olan tüm sistemlerin izlenmesi, operasyonel işlerin yürütülmesi ve ÖKC TSM operasyonlarının sürekliliğinin sağlanmasından sorumludur.
- **Terminal Operasyonu**
 - Yönetici
 - Terminal Operasyon Elemanları

20.4 Uygulama Geliştirme Grubu:

(Grupta en az 5 kişi olmalıdır.)

Uygulama geliştirme ve destek için dışarıdan hizmet alımı yöntemi benimsenmeli ya da biri teknik yönetici olmak üzere en az 5 kişilik yazılım geliştirme ekibi görevlendirilmelidir.

21. ÖKC TSM’lerinin Periyodik Denetimi

ÖKC TSM’lerinin, bilgi sistemlerinin ve bu Kılavuzun gereksinimler (güvenlik ve sistem gereksinim) bölümlerinde belirtilen hükümlere uyum durumunun devamının tespit edilmesi

amacıyla, düzenli olarak (üç yılda en az 1 defa) ya da Başkanlık talebiyle istendiği zaman denetim yapılır.

ÖKC TSM'lerinin bilgi sistemleri denetimi ve denetim sonuçlarının Başkanlığa raporlanması bu Kılavuzdaki tanımla sınırlı olmak üzere BSDHY ile belirlenen usul ve esaslar çerçevesinde, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş bağımsız denetim kuruluşlarınca gerçekleştirilir.

BSDHY ile belirlenen usul ve esaslar bu Kılavuz çerçevesinde uygulanırken BSDHY'de geçen “banka” ve “denetlenen” ifadeleri ÖKC TSM'lerini, “Bilgi Sistemleri Denetimi” ifadesi de ÖKC TSM'leri üzerinde bu Kılavuzda tanımlanan denetimi ifade eder.

ÖKC TSM'lerinde gerçekleştirilecek denetim faaliyetlerine ilişkin detaylar bu Kılavuzun IV üncü bölümünde açıklanmıştır.

22. Başkanlık Uyarı Mekanizmaları

ÖKC TSM'lerinden bazı durumlarda BİM'e ulaşması gerekebilir. Bu konuda aciliyet durumlarına göre yazılı, e-mail, telefon, faks, SMS vb. yoluyla iletişim kurulması mümkün olduğu gibi otomatik işleyen bazı altyapılar da kullanılabilecektir. Üretilen YN Pompa ÖKC'lerin kaydedilmesi, statülerinin (kullanıma hazır, aktif, kapalı, devir, hurdaya ayrılma vb.) güncellenmesi, Başkanlık tarafından yayımlanan “Yeni Nesil Akaryakıt Pompa ÖKC'lere Ait Elektronik Kayıt, Aktivasyon ve Yetkili Servis Listeleri Teknik Kılavuzu”na uygun olarak gerçekleştirilecektir. ÖKC TSM'leri tarafından tespit edilen bir atak ya da önemli bir durumun BİM'e bildirilmesi için, erişim bilgileri Başkanlık tarafından ayrıca duyurulacak olan İstihbarat Web Servisi kullanılacaktır. Aynı zamanda, BİM'den ÖKC TSM'lerine, cihazlar ve ÖKC TSM'leri hakkında bilgilendirmeler de, “Yeni Nesil Akaryakıt Pompa ÖKC'lere Ait Elektronik Kayıt, Aktivasyon Ve Yetkili Servis Listeleri Teknik Kılavuzu” nda yer alan esaslara göre yapılabileceği gibi Başkanlık tarafından ilan edilecek farklı mekanizmalar da kullanılabilecektir.

Bu mekanizmalar online veya batch entegrasyon yöntemlerinden biri ile olabilecektir. Online ya da batch entegrasyon formatı ve kuralları daha sonra detaylı olarak iletilecektir.

BÖLÜM III

YENİ NESİL AKARYAKIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT ÖKC TSM'LERİ ONAY VE TEST BAŞVURU AKIŞLARI

23. Onay ve Test Başvuru Yönetimi

Bu bölümde ÖKC TSM başvurularına ilişkin olarak Başkanlığa yapılan başvuruların iş akışları düzenlenmiştir.

ÖKC TSM'nin başvuru, test ve onay denetimi, sadece yetkili ÖKC onayı almış veya başvuruda bulunmuş firmalar için yapılması zorunlu olup ÖKC Üreticisi olmaksızın yapılan ÖKC TSM başvuruları dikkate alınmayacaktır. YN Pompa ÖKC onayı için Başkanlığa yapılacak yazılı müracaat, cihaz ve TSM onay başvurusu olmak üzere iki ayrı teknik dosya ile yapılmalıdır.

23.1 ÖKC TSM Başvurusunda Sağlanacak Belgeler

ÖKC TSM başvurularında aşağıdaki belgelerin teslim edilmesi zorunludur.

- a. ÖKC TSM Başvuru Formu (EK-2)
- b. BDK ile yapılan “Onay Denetimi” sözleşmesi
- c. PCI-DSS Payment Card Industry Data Security Standard Onay Belgesi
AOC (Attestation of Compliance for Onsite Assessments).
- ç. ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi
- d. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi
- e. ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi
- f. Teknik Rapor Dokümanı (YN Pompa ÖKC TSM Teknik Kılavuzu, madde 6/2)
- g. Güvence ve Denetim Rapor Dokümanı (YN Pompa ÖKC TSM Teknik Kılavuzu, madde 10/8)
Daha önceden ÖKC TSM hizmeti vermeye başlamış ve bankalara bütünleşik cihazlarından (EFT POS) mesaj göndermeye başlamış ÖKC TSM'leri için geçmişe ait son 6 aya ait aylık bazda kullanılabilirlik oranı raporu. Tek bir banka için verilmesi yeterlidir.
- ğ. İş Sürekliliği Planı Dokümanı (YN Pompa ÖKC TSM Teknik Kılavuzu, madde 10/1)
- h. **ÖKC Üreticisi – ÖKC TSM Yetki Sorumluluk Anlaşma ve Dokümanları:** ÖKC Üreticisi ile ÖKC TSM'si arasındaki yetki ve sorumluluklara ilişkin anlaşma ve ekleri.

1. **İç Kontrol ve İç Denetim Dokümanları:** Verileri yöneten yazılım, donanım ve kişiler (veya roller) arası iletişim ve süreçlerin uygunluğunun temini için yazılmış iç kontrol ve iç denetim prensipleri dokümanı.
- i. **Gün içi ve Gün sonu Süreçleri Dokümanları:** ÖKC Üreticisi için gün içi ve gün sonunda yapılan bütün işlerin (uygulamalar, dosya alışverişleri, entegrasyonlar vb.) adım adım özetinin anlatıldığı tarif dokümanı.
- j. **İkincil Merkez Anlaşması:** ÖKC TSM ikincil merkezi barındırma hizmeti olarak başka bir firmadan alıyorsa, alındığını gösteren sözleşme kapsamını, sözleşme tarihini, sözleşme başlama – bitiş tarihlerini ve süresini gösteren belgeler / sözleşme ön yüzü.
- k. **Diğer Anlaşmalar ve Dokümanlar:** ÖKC TSM hizmeti faaliyetlerine ilişkin harici kurumlarla yapılan diğer mevcuttaki anlaşmalar veya sözleşmeleri tarif eden doküman. (Örneğin: Katma değerli servisler ile ilgili sözleşmeler vb.)

23.2 ÖKC TSM Denetim ve Onay Süreçleri

ÖKC Üreticileri cihazları için cihaz onayını aldıktan sonra cihazlarının yönetiminden sorumlu olacak ÖKC TSM başvurusu için EK-2’de yer alan (**ÖKC TSM BAŞVURU FORMU**) ve 23.1 başlığında yer alan belgeleri tamamlayarak Başkanlığa yazılı olarak başvurur. Başkanlık tarafından ön kontrolleri yapılan başvuru formu ve ekleri uygun görüldüğü takdirde, onay denetimi sürecinin başlatılabileceğine ilişkin ÖKC TSM başvuru sahibine yazılı olarak bildirim yapılır.

ÖKC TSM’sinin gerekli şartları haiz olup olmadığının tespiti için onay denetimi, BSDHY kapsamında yetkilendirilmiş veya izin verilmiş BDK veya TÜBİTAK tarafından gerçekleştirilir.

ÖKC Üreticileri ÖKC TSM’lerinin bu Kılavuza göre yapılacak test, denetim ve değerlendirme faaliyetlerini BDK ya da TÜBİTAK’a yaptırılmasını başvuru sırasında belirterek tercih edebilirler. İlgili liste <https://ynokc.gib.gov.tr/> internet adresinde yayımlanır.

TÜBİTAK onay denetiminin bir veya daha fazla bölümünü harici firmalara (Başkanlıkça ÖKC TSM’lerinin denetimi hususunda yetkilendirilen Bağımsız Denetim Kuruluşları dahil) yaptırabilir.

Onay denetiminin kapsamı bu Kılavuzda detaylı açıklanmaktadır. Onay denetiminde gerçekleştirilecek test, değerlendirme ve denetim faaliyetlerine ilişkin tanzim edilecek raporun

formatı EK-3’de yer almaktadır. Onay denetimi raporu TÜBİTAK tarafından bu Kılavuza uygunluk yönünden kontrol edilecek ve TÜBİTAK tarafından kontrolü sağlanmış şekilde Başkanlık ile paylaşılacaktır.

TÜBİTAK, söz konusu onay denetim raporunu, bu Kılavuza uygun olarak hazırlandığını belirten dokümanla (yazı veya bir rapor şeklinde) birlikte Başkanlığa gönderir. Onay raporu olumlu olarak kabul edilen başvurularda Başkanlık olumlu değerlendirme yazısını firmaya bildirir. Onay denetimi başarılı sonuçlanan firmalar ÖKC TSM uçtan uca test işlemlerine başlayabilmek için Başkanlığa başvuruda bulunur.

GMP dokümanına uygun olarak hazırlanan uçtan uca test senaryoları Başkanlık tarafından başvuru ön kabulünden sonra paylaşılır.

Başkanlık tarafından yayımlanan “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara ait ÖKC TSM Teknik Kılavuzu” nda belirtilen ve her 3 yılda 1 yapılması gereken Bilgi Sistemleri Denetiminin ilki onay denetimi kapsamında yapılmalıdır.

ÖKC TSM başvurularının; yetkili ÖKC firması ve ilgili ÖKC firmasına ait gerekli onayları almış bulunan veya onay başvurusu TÜBİTAK nezdinde devam eden YN Pompa ÖKC modelleri bazında yapılması gerekmektedir. Bir başvuruda, aynı ÖKC firmasına ait birden fazla YN Pompa ÖKC modeline de yer verilmesi mümkündür. ÖKC TSM onay denetiminde, Güvenli Haberleşme Denetim adımları her bir cihaz modeli için dokümanda belirtilen tekrar kurallarına uygun tatbik olunmalıdır.

23.3 Dış Hizmet Sağlayıcılı ÖKC TSM Denetim ve Onay Süreçleri

ÖKC Üreticileri, ÖKC TSM’sine ait sunulması gereken hizmet altyapılarını kısmen veya tamamen bir DHS’den temin etmesi durumunda; ÖKC Üreticisine ve DHS’ya ait ÖKC TSM sistem unsurlarının niteliğine bağlı ve bu Kılavuzda belirtilen gereksinim unsurlarının (bilgi sistemleri ve güvenli haberleşme gereksinimleri) karşılandığını temin etmelidirler. Söz konusu unsurlara ilişkin sorumluluk müşterek ve müteselsil olup, DHS ile birlikte ÖKC Üreticilerine aittir.

ÖKC TSM’sine ilişkin hizmetlerin kısmen veya tamamen bir DHS’den temin edilmesi halinde; ÖKC TSM Başvurusunda (Ek-2) DHS’den temin edilen hizmet unsurları detaylı olarak belirtilmeli ve bu hizmetlerin niteliğine bağlı olarak gerekli ek ve tevsik edici bilgi ve belgeler

başvuru formunda sunulmalıdır. ÖKC TSM'sine ilişkin test ve onay süreçlerinde DHS'den temin edilen bu hizmet unsurları da test, denetim ve değerlendirmeye tabi tutulmalıdır.

Bu aşamadan sonra yapılması gereken iş ve işlemler ile sertifikasyon süreçleri bu Kılavuzun 23.2 bölümünde belirtilen şekilde tamamlanır.

DHS'li ÖKC TSM başvurularının; ÖKC TSM'nin başvuru, test ve onay denetimi, sadece yetkili ÖKC onayı almış veya başvuruda bulunmuş firmalar için yapılması zorunlu olup ÖKC Üreticisi olmaksızın yapılan ÖKC TSM başvuruları dikkate alınmayacaktır. YN Pompa ÖKC onayı için Başkanlığa yapılacak yazılı müracaat, cihaz ve TSM onay başvurusu olmak üzere iki ayrı teknik dosya ile yapılmalıdır. Bir başvuruda birden fazla YN Pompa ÖKC modeline yer verilmesi mümkün olup, ÖKC TSM onay denetiminde, Güvenli Haberleşme Denetim adımları her bir cihaz için dokümanda belirtilen tekrar kurallarına uygun tatbik olunmalıdır.

DHS'ler tarafından sunulan ÖKC TSM hizmet unsurlarının, sistemlerin münhasırlığı gereği; birlikte çalışacakları her farklı Üretici firma için ayrı ayrı test, denetim ve değerlendirme süreçlerine tabi tutulması gerekmektedir.

23.4 Onay Denetimi Sonrasında Test Başvuruları ve Gerçek Ortama Geçiş

Onay denetimi raporu ve TÜBİTAK format kontrolü sonrasında Başkanlık tarafından olumlu değerlendirilen firmalar için ÖKC TSM'lerinin uçtan uca test süreci, firmanın başvurusu akabinde Başkanlık tarafından firmalara bildirilen test takvimine göre yürütülecektir.

Uçtan uca test senaryolarının firmaların başvurusunda belirtilen her bir YN Pompa ÖKC marka modeli için tekrar edilmesi gereklidir.

ÖKC TSM uçtan uca test süreçlerini başarıyla tamamlayan firmalar Başkanlık tarafından ÖKC TSM olarak onaylanır, ÖKC TSM onayı yazılı olarak ÖKC Üreticisine bildirilir. Başkanlık, ÖKC Üreticilerine ait sadece belli bir YN Pompa ÖKC kümesinin gerçek (canlı) ortama bağlanmasını (pilot süreci) tercih edebilir. Bu durumda pilot süreci tamamlandıktan sonra tüm YN Pompa ÖKC'ler gerçek ortama bağlanmaya başlayabilir.

BÖLÜM IV

ÖKC TSM'LERİNDE GERÇEKLEŞTİRİLECEK DENETİM FAALİYETLERİ

24. ÖKC TSM'lerinde Gerçekleştirilecek Onay Denetiminin Kapsamı

ÖKC TSM'lerinde gerçekleştirilecek onay denetiminin kapsamı, ÖKC TSM olmak üzere Başkanlığa başvuruda bulunan ÖKC Üreticilerinin kurmuş oldukları sistemin Başkanlık tarafından talep edilen gerekli şartları haiz olup olmadığının tespiti için gerçekleştirilen denetim sürecidir.

ÖKC TSM'lerinde gerçekleştirilecek onay denetim faaliyetleri esas itibarıyla “Bilgi Sistemleri Denetimi” ve “Güvenli Haberleşme Denetimi” olarak isimlendirilen iki kısımdan oluşmaktadır.

24.1 ÖKC TSM'leri Bilgi Sistemleri Denetimi

ÖKC TSM'leri bilgi sistemleri denetimi, ÖKC TSM'lerinde yürütülen işlemlerin; Başkanlıkça yayımlanan/paylaşılan ve ÖKC TSM'lerini doğrudan veya dolaylı olarak etki eden teknik kılavuzlar ile BSDHY'de belirtilen usul ve esaslar uygunluğuna yönelik yapılan denetim faaliyetleridir.

“Bilgi Sistemleri Denetimi” kapsamında; YN Pompa ÖKC verisini ve kural koyucular tarafından hassas veri olarak kabul edilen verileri yöneten kişiler, süreçler, yazılımlar, donanımlar ile bu kapsamda tesis edilen iş süreçleri ve iç kontrollerin değerlendirilmesinde, Başkanlık tarafından yayımlanan “Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Bilgi Sistemleri Denetimi Adımları Kılavuzu” nda yer alan kontrol sınıfları çalıştırılmalıdır.

ÖKC TSM'sinin, Başkanlık isterleri olan teknik kılavuzlara uygunluk değerlendirmesinde çalıştırılacak kontrol sınıfları aşağıda belirtilmiştir.

1. TSM_SER: Uluslararası Sertifikasyon Raporları ve Denetim Talepleri Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM'lerinin sağlaması gereken uluslararası standartlara ait sertifikasyon süreçlerinin çıktıları ile ÖKC TSM'lerinin rutin olarak sağlaması gereken denetim süreçlerinin varlığının ve uygunluğunun kontrol edilmesini amaçlamaktadır.

2. TSM_SIS : Sistem ve Güvenlik Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM'lerinin uyması gereken altyapı, sistem mimarisi, münhasırlık kuralları ile veri merkezi iş sürekliliğinin temini, gerekli güvenlik ve risk değerlendirme süreçlerinin oluşturulması ve işletilmesi, yazılım değişikliklerinin yönetimi, gerçekleştirilen işlemlerin denetim izlerinin sağlanması, DHS ile çalışılması durumunda sağlanması gereken hususi gerekliliklerin kontrol edilmesini amaçlamaktadır.

3. TSM_ILT : Paydaş İletişimi ve İş Kurgusu Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM'lerinin YN Pompa ÖKC yönetimi çerçevesinde iletişim içerisinde olduğu, ÖKC Üreticisi, üye işyeri anlaşması yapan kuruluşlar ve katma değerli hizmet sağlayıcılar ile ilişki yönetiminin gerekliliklere uygunluğunun kontrol edilmesini amaçlamaktadır.

4. TSM_OKC : Güvenli Yazılım Yükleme ve Mesaj Yönetim Değerlendirme Sınıfı

Bu değerlendirme sınıfı, ÖKC TSM'lerinin YN Pompa ÖKC üzerinde çalışan mali uygulama, üye işyerleri anlaşması yapan kuruluşlara ait uygulama veya katma değerli uygulama yazılımlarının ayrıca YN Pompa ÖKC parametrelerinin cihaza yüklenmesi ve versiyon takibinin gerekliliklere uygun sağlandığının ve ÖKC mesajlarının istelere uygun yönetildiğinin kontrol edilmesini amaçlamaktadır.

Söz konusu denetim adımları ile ilgili olarak, denetim faaliyetlerini yürütecek bağımsız denetim kuruluşlarının Gelir İdaresi Başkanlığı koordinatörlüğünde sunulan eğitim faaliyetine katılması zorunludur.

Gerçekleştirilen denetim sonucunda BSDHY'nin 5 inci, 7 nci ve 8 inci maddelerinde belirtilen hükümler çerçevesinde, BSDHY'nin 34 üncü maddesinde belirtilen şekilde denetim mektubu düzenlenir. Denetim mektubu düzenlenirken metinde EK-1'de yer verilen ifade değişiklikleri uygulanır. Denetim mektubu, hazırlanan denetim raporu içerisinde yer alır.

24.2 ÖKC TSM'leri Güvenli Haberleşme Denetimi

ÖKC TSM'leri güvenli haberleşme denetimi, ÖKC TSM'leri güvenli haberleşme denetimi, ÖKC TSM'lerinde yürütülen işlemlerin; Başkanlıkça yayımlanan/paylaşılan ve ÖKC TSM'lerine

doğrudan veya dolaylı olarak etki eden mesajlaşma protokolü dokümanı (GMP, GMP-3 vb.) isterlerine uygunluğuna yönelik yapılan denetim faaliyetleridir.

Başkanlık isterleri olan mesajlaşma protokolü dokümanlarına uygunluk değerlendirmesinde çalıştırılacak kontrol sınıfları aşağıda belirtilmiştir.

Söz konusu denetim kılavuzunda belirtilen denetim işlem adımları ve detayları ile ilgili olarak, denetim faaliyetlerini yürütecek bağımsız denetim kuruluşlarının Başkanlık tarafından sunulan eğitim faaliyetine katılması zorunludur.

Bu denetim kapsamında sınıflar itibariyle aşağıdaki denetim faaliyetleri yürütülecektir.

1. SSL_CON : ÖKC TSM SSL Konfigürasyonu Değerlendirme Sınıfı

Bu değerlendirme sınıfı, YN Pompa ÖKC ile ÖKC TSM arasındaki veri transferinin güvenliğini sağlamak için kurulan güvenli bağlantının (SSL CA) ÖKC TSM yapılandırma özelliklerinin tespit edilmesini ve uygunluğunun kontrol edilmesini amaçlamaktadır.

2. SSL_COM : ÖKC TSM - YN Pompa ÖKC SSL Haberleşmesi Değerlendirme Sınıfı

Bu değerlendirme sınıfı, YN Pompa ÖKC ile ÖKC TSM arasında kurulacak güvenli bağlantının (SSL CA) haberleşme güvenliği özelliklerinin GMP dokümanına uygunluğunun kontrol edilmesini amaçlamaktadır.

3. SSL_CEV : SSL Sertifika Doğrulama Değerlendirme Sınıfı

Bu değerlendirme sınıfı, YN Pompa ÖKC ile ÖKC TSM arasında kurulacak güvenli bağlantı esnasında kullanılan sertifikaların uygunluğunun kontrol edilmesini amaçlamaktadır.

25. ÖKC TSM'lerinde Gerçekleştirilecek Periyodik Denetiminin Kapsamı

ÖKC TSM'lerinde gerçekleştirilecek periyodik denetiminin kapsamı, ÖKC TSM'sinin periyodik denetimi; Başkanlık tarafından verilen ÖKC TSM onay tarihinden itibaren her 3 yılda bir yapılması gereken denetim sürecini ifade eder. Periyodik denetim raporunun düzenlendiği tarihten itibaren en geç 30 gün içerisinde Başkanlığa teslim edilmesi gerekmektedir. ÖKC TSM'lerinin onay denetimi sürecinde tanzim edilen ve Başkanlık tarafından uygun bulunan raporlar, periyodik denetim raporu yerine geçer. 3 yıllık periyot, onay denetim raporunun düzenlendiği tarihten itibaren başlar.

ÖKC TSM’lerinde gerçekleştirilecek periyodik denetim faaliyetleri, ÖKC TSM onay denetiminde de yer alan “Bilgi Sistemleri Denetimi” sürecini kapsamaktadır. Bu sürece ilişkin kapsam bu Kılavuzda detaylı olarak açıklanmakta olup, süreç aynı şekilde işletilecektir.

Onay denetimi sonrasında, GMP dokümanlarında gerçekleştirilecek düzenlemelere bağlı olarak Başkanlık, bu Kılavuzda açıklanan “Güvenli Haberleşme Denetimi”nin tekrar edilmesini talep edebilir.

26. ÖKC TSM Denetimine İlişkin Düzenlenen Raporların Formatı

ÖKC TSM’lerinde gerçekleştirilen denetim faaliyetleri sonucunda TÜBİTAK veya BDK tarafından düzenlenecek “YN ÖKC TSM ONAY DENETİM RAPORU ” nun asgari formatı Ek-3’de belirtilmiştir. İlgili rapor, TÜBİTAK tarafından gerekli format kontrolü yapıldığına ilişkin üst yazı ekinde olmak şartıyla Başkanlık tarafından kabul edilecektir.

Başkanlık tarafından verilen ÖKC TSM onay tarihinden itibaren 3 yılda bir gerçekleştirilecek “Bilgi Sistemleri Denetimi” sonrasında düzenlenecek “YN Pompa ÖKC TSM BİLGİ SİSTEMİ DENETİM RAPORU ”nun asgari formatı EK-4A’da belirtilmiştir. Başkanlığa başvuru yapan ancak ön kabul verilmeyen firmalar için “Bilgi Sistemleri Denetimi” zorunlu olarak gerçekleştirilmeli ve EK-4A’ya uygun formatta denetim raporu tanzim edilmelidir. İlgili raporlar doğrudan Başkanlık tarafından kabul edilecektir. 3 yıllık periyot, onay denetim raporunun düzenlendiği tarihten itibaren başlar.

Başkanlık tarafından mesajlaşma protokollerinde gerçekleştirilecek düzenlemeler dolayısı ile “Güvenli Haberleşme Denetimi”nin tekrar edilmesinin talep edildiği durumda; “Güvenli Haberleşme Denetimi” sonrasında TÜBİTAK veya BDK tarafından düzenlenecek “YN Pompa ÖKC TSM GÜVENLİ HABERLEŞME DENETİM RAPORU ” nun asgari formatı EK-4B’de belirtilmiştir. İlgili rapor, TÜBİTAK tarafından gerekli format kontrolü yapıldığına ilişkin üst yazı ekinde olmak şartıyla, Başkanlık tarafından kabul edilecektir.

27. KILAVUZ EKLERİ

EK-1: Denetim Mektubu Oluşturulurken Metinde Değiştirilmesi Gereken Hususlar:

Denetim mektubu düzenlenirken "13.01.2010 tarih 27461 sayılı Resmi Gazete’de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik", "28.06.2012 tarih ve 28337 sayılı Resmi Gazete’de yayımlanan Bankaların İç Sistemleri Hakkında Yönetmelik ile 14.09.2007 tarih ve 26643 sayılı Resmi Gazete’de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ", "01.11.2006 tarih ve 26333 sayılı Resmi Gazete’de yayımlanan Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" ile "13.01.2010 tarih ve 27461 sayılı Resmi Gazete’de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik", "28.06.2012 tarih ve 28337 sayılı Resmi Gazete’de yayımlanan Bankaların İç Sistemleri Hakkında Yönetmelik’in “İç Kontrol Sistemi” başlıklı İkinci Kısım” ile "14.09.2007 tarih ve 26643 sayılı Resmi Gazete’de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" ifadeleri yerine **"Yeni Nesil Akaryakıt Pompa Ödeme Kaydedici Cihazlara Ait ÖKC TSM Teknik Kılavuzu"** ifadesi ve "(bilgi sistemleri)* bankacılık süreçleri" ve " bilgi sistemleri ile bankacılık süreçleri" ifadeleri yerine **"YN Pompa ÖKC TSM’leri Bilgi Sistemleri"** ifadesi kullanılır.

EK-2: ÖKC TSM Başvuru Formu

YENİ NESİL AKARYAKIT POMPA ÖDEME KAYDEDİCİ CİHAZLARA AİT TSM BAŞVURU FORMU	
A. ÖKC TSM TÜRÜ	
ÜRETİCİ ÖKC TSM (Tüm altyapı hizmetinin ÖKC Üreticisine ait olması hali)	☐
DIŞ HİZMET SAĞLAYICILI ÖKC TSM (ÖKC TSM altyapılarına ilişkin kısmen veya tamamen bir dış hizmet sağlayıcıdan yararlanılması hali)	☐
ORTAK KULLANIMLI ÖKC TSM (ÖKC Üreticilerinin ÖKC TSM altyapısını birlikte ortaklaşa olarak kullanabilmeleri YN Pompa ÖKC TSM TK Madde 19/4)	☐
B. ÖKC ÜRETİCİ KURUM BİLGİLERİ	
KURUM ÜNVANI	
İRTİBAT KURULACAK KİŞİ ADI-SOYADI	
BÖLÜM/GÖREV/ÜNVAN	
İrtibat Tel No	
İrtibat GSM No	
e-mail	
Adresi	
C. DIŞ HİZMET SAĞLAYICISI BİLGİLERİ (Kısmen veya tamamen bir dış hizmet sağlayıcısından yararlanılması halinde)	
KURUM ÜNVANI	
İRTİBAT KURULACAK KİŞİ ADI-SOYADI	
BÖLÜM/GÖREV/ÜNVAN	
İrtibat Tel No	
İrtibat GSM No	
e-mail	
Adresi	

D. ÖKC TSM BİRİNCİL MERKEZ BİLGİLERİ			
İRTİBAT KURULACAK KİŞİ ADI-SOYADI			
BÖLÜM/GÖREV/ÜNVAN			
İrtibat Tel No			
İrtibat GSM No			
e-mail			
ÖKC TSM BİRİNCİL MERKEZİN ADRESİ:			
E. ÖKC TSM İKİNCİL MERKEZ BİLGİLERİ			
İRTİBAT KURULACAK KİŞİ ADI-SOYADI			
BÖLÜM/GÖREV/ÜNVAN			
İrtibat Tel No			
İrtibat GSM No			
e-mail			
ÖKC TSM İKİNCİL MERKEZİN ADRESİ:			
F. ÖKC TSM HİZMETİ VERİLECEK YN POMPA ÖKC'LERE AİT BİLGİLER (*)			
SIRA NO	MARKA	MODEL	TÜRÜ (EFT-POS ÖZELLİKLİ/BASİT-BİLGİSAYAR BAĞLANTILI)
1			
2			
(*) ÖKC TSM Hizmeti verilecek her marka ve model ÖKC için ilgili satırlar çoklanacaktır. ÖKC TSM hizmetine daha sonradan dahil edilmesi talep edilen ÖKC marka, model ve türüne ilişkin bildirimlerin yazılı olarak GİB'e yapılması gerekmektedir.			

G. BAŞVURU FORMU EKLERİ			
	ÖKC Üreticisine Ait	DHS'ye Ait	Ortak Kullanımlı TSM Hizmet Veren
1- BDK ONAY DENETİM SÖZLEŞMESİ	☐	☐	☐
2- PCI DSS	☐	☐	☐
3- ISO/IEC 20000	☐	☐	☐
4- ISO/IEC 27001	☐	☐	☐
5- ISO 22301	☐	☐	☐
6- TEKNİK RAPOR	☐	☐	☐
7- GÜVENÇE VE DENETİM RAPORU	☐	☐	☐
8- İŞ SÜREKLİLİĞİ DOKÜMANI	☐	☐	☐
9- ÖKC ÜRETİCİSİ TSM YETKİ SORUMLULUK ANLAŞMA VE DOKÜMANLARI	☐	☐	☐
10- İÇ KONTROL VE İÇ DENETİM DOKÜMANLARI	☐	☐	☐
11- GÜN İÇİ VE GÜN SONU SÜREÇLERİ DOKÜMANLARI	☐	☐	☐
12- DHS HİZMET SÖZLEŞMESİ	☐	☐	☐
13- İKİNCİL MERKEZ ANLAŞMASI	☐	☐	☐
14- ÜRETİCİ KURUM İMZA SİRKÜLERİ	☐	☐	☐
15- DHS KURUM İMZA SİRKÜLERİ	☐	☐	☐
H- DIŞ HİZMET SAĞLAYICIDAN TEMİN EDİLEN HİZMET UNSURLARINA İLİŞKİN BİLGİLER			
ÖKC Üreticisinin; ÖKC TSM'e ilişkin hizmetlerden kısmen veya tamamen bir dış hizmet sağlayıcıdan yararlanması halinde; yararlanılan hizmet unsurları detaylı olarak açıklanacak ve hizmetin niteliğine bağlı olarak dış hizmet sağlayıcı tarafından temin edilen tevsik edici bilgi ve belgeler (sertifikalar, sözleşmeler vb.) başvuru formu ekinde Başkanlığa ibraz edilecektir.			
I. DİĞER ANLAŞMA VE DOKÜMANLARA İLİŞKİN AÇIKLAMALAR			
Bu form ve eklerinde kurumumuza ilişkin yer alan bilgi ve belgelerin doğruluğunu beyan ve taahhüt ederiz.			

ÖKC ÜRETİCİSİ KURUM UNVANI	DIŞ HİZMET SAĞLAYICI KURUM UNVANI
Yetkili Adı-Soyadı	Yetkili Adı-Soyadı
İmza	İmza
Tarih:	Tarih:

YN Pompa ÖKC TSM Teknik Kılavuzu 19/4 Madde Kapsamında (Ortak TSM Kullanımı) Doldurulacak Bölüm

Bu form ve eklerinde kurumumuza ilişkin yer alan bilgi ve belgelerin doğruluğunu beyan ve taahhüt ederiz.	
ÖKC ÜRETİCİSİ (HİZMET VEREN) KURUM UNVANI	ÖKC ÜRETİCİSİ (HİZMET ALAN) KURUM UNVANI
Yetkili Adı-Soyadı	Yetkili Adı-Soyadı
İmza	İmza
Tarih:	Tarih:

EK-3 : “ÖKC TSM Onay Denetim Raporu Formatı”

KAPAK

DİZİN

I- GENEL BİLGİ

Denetim faaliyeti gerçekleştirilen ÖKC TSM'ine ilişkin genel bilgiler (ÖKC TSM hizmeti verilecek ÖKC firmasının ünvanı, cihaz marka, model ve türü yazılacaktır.

II- ÖKC TSM'SİNDE GERÇEKLEŞTİRİLEN BİLGİ SİSTEMLERİ DENETİMİ FAALİYETLERİ

III- ÖKC TSM'İNDE GERÇEKLEŞTİRİLEN GÜVENLİ HABERLEŞME DENETİMİ FAALİYETLERİ

IV- SONUÇ

Raporun önceki bölümlerinde elde edilen bulgular çerçevesinde, denetimi yürütülen ÖKC TSM Başvurusunun onayını uygun olup olmadığı hakkında görüş bildirilecektir.

EK-4A : “ÖKC TSM Periyodik Denetim Raporu Formatı

KAPAK

DİZİN

I- GENEL BİLGİ

Denetim faaliyeti gerçekleştirilen ÖKC TSM'ine ilişkin genel bilgiler (ÖKC TSM hizmeti verilecek ÖKC firmasının ünvanı, cihaz marka, model ve türü yazılacaktır.

II- ÖKC TSM'İNDE GERÇEKLEŞTİRİLEN BİLGİ SİSTEMLERİ DENETİMİ FAALİYETLERİ

III- SONUÇ

Raporun önceki bölümlerinde elde edilen bulgular çerçevesinde, denetimi yürütülen ÖKC TSM Başvurusunun Periyodik Denetim değerlendirmesinin uygun olup olmadığı hakkında görüş bildirilecektir.

EK-4B: “ÖKC TSM Güncelleme Denetimi Rapor Formatı

KAPAK

DİZİN

I- GENEL BİLGİ

Denetim faaliyeti gerçekleştirilen ÖKC TSM'ine ilişkin genel bilgiler (ÖKC TSM hizmeti verilecek ÖKC firmasının ünvanı, cihaz marka, model ve türü yazılacaktır.

II- ÖKC TSM'İNDE GÜVENLİ HABERLEŞME DENETİMİ FAALİYETLERİ

III- SONUÇ

Raporun önceki bölümlerinde elde edilen bulgular çerçevesinde, denetimi yürütülen ÖKC TSM Başvurusunun güncellenen mesajlaşma protokol dokümanlarına uygun denetim değerlendirmesinin uygun olup olmadığı hakkında görüş bildirilecektir.

REFERANSLAR

- [1] <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>
- [2] http://www.iso.org/iso/catalogue_detail?csnumber=50038