

11/6/2024 tarihli ve 32573 sayılı Resmî Gazete’de yayımlanan “Nükleer Tesislerin ve Nükleer Maddelerin Emniyetine İlişkin Yönetmelik” kapsamında Nükleer Düzenleme Kurumuna sunulması gereken

İÇ DENETİM RAPORU

[İç Denetim Periyodu:/.../20... -/...../20...]

İç Denetimi Gerçekleştiren Yer

Tesis adı	
Tesis kodu	
Tesis iletişim bilgileri	
İç denetim tarihi	

Tesis Sorumlusu

Tesis Sorumlusunun bilgileri	Adı Soyadı	
	Ünvanı	
Tesis Sorumlusunun iletişim bilgileri	Telefon	
	Faks	
	E-posta	
Açıklama (bir önceki iç denetimden bu yana Tesis Sorumlusunda ya da iletişim bilgilerinde vb. değişiklik olduysa belirtiniz)		

Emniyet Personeli

Emniyet Personelinin bilgileri	Adı Soyadı	
	Ünvanı	
Emniyet Personelinin iletişim bilgileri	Telefon	
	Faks	
	E-posta	
Açıklama (bir önceki iç denetimden bu yana emniyet personelinde ya da iletişim bilgilerinde vb. değişiklik olduysa belirtiniz)		

1. Emniyet Fonksiyonlarının Denetlenmesi

a. Erişim kontrolü

Emniyet alanlarının tanımlanmasında bir değişiklik yapıldı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Emniyet alanlarına erişim kontrolüne ilişkin süreçlerde (kartlı sistem, PIN kullanımı vb.) bir değişiklik yapıldı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Erişim yetkilendirme süreçlerinde (anahtarların doğrulanması, yaka kartlarının ve erişim kayıtlarının korunması vb.) bir değişiklik yapıldı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Yasak maddeleri tespit etmeye yönelik önlemler ve kayıtlar gözden geçirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Personel ve ziyaretçiler için uygulanan erişim kontrol prosedürü ve yasak maddeleri tespit etme sistemi test edildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgisayarlarda ve bilgisayar tabanlı sistemlerde erişim kontrol mekanizmaları yeterli şekilde uygulanmakta mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Erişim noktalarının kontrolü gerçekleştirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Erişim kontrollerine ilişkin yapılan değişiklikler kayıt altına alınmakta mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Açıklama*		

b. Tespit etme

Tespit etme sistemi bütünlük ve dengeli mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Algılayıcıların işlevselliği doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Yetkisiz eylemleri tespit edecek personelin sorumlu olduğu prosedürler ve sistemi test etme süreçleri gözlemlendi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Algılayıcıların test, alarm, log ve bakım kayıtları gözden geçirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Radyoaktif madde tespit etme cihazları test edildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgisayar ve bilgisayar tabanlı sistemlerde güncel yamaların yapıldığı ve imza veri tabanının güncel olduğu zararlı yazılımdan korunma uygulamaları kullanılmakta mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Zararlı yazılım taramaları prosedürlere uygun sıklıkta ve düzenli olarak yapılmakta mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Açıklama*		

c. Alarm değerlendirme

Tesisin alarm değerlendirme düzenlemeleri gözden geçirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Alarm değerlendirme prosedürleri gözden geçirildi mi? Bu bağlamda aydınlatmanın yeterli, monitörlerin sürekli gözlem altında olması, kapalı devre kamera sistemini (CCTV) ve alarmları değerlendiren personelin etkin çalışması doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Açıklama*		

d. Geciktirme

Yetkisiz eylemleri geciktirme önlemlerinin, fiziksel bariyerlerin dereceli yaklaşıma uygun olarak ve dengeli yerleştirilmesi gözden geçirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Kullanılan fiziksel bariyerler tanımlandı ve fiziksel bariyerlerin yeterliliği ve geciktirme süreleri gözden geçirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Geciktirme önlemlerinin sürekliliği (kestirme yolların, korunmasız açıklıkların, boşlukların olmaması vb.) doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Kapılara uygun nitelikte giriş ve kilitlerin kullanılması gibi geciktirmenin dengeli sağlanmasına yönelik uygulamalar gözlemlendi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Açıklama*		

e. Müdahale

Müdahale kabiliyeti gözden geçirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır	
Özel güvenlik görevlileri için belirtilen hususlar emniyet planına uygun mu?	1. Vardiyada görevli personel sayısı	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	2. Donanım	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	3. Eğitim	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	4. Etkinlik değerlendirmeleri için performans değerlendirmesi	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	5. Müdahale prosedürleri	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	6. Farklı tespit etme noktaları için müdahale sürelerine ilişkin performans değerlendirmesi	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	7. İletişim sistemleri	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır

	8. Devriye periyodu	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Kolluk kuvvetlerinin müdahalesi için hazırlıklar iş birliği protokolüne uygun mu?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Kolluk kuvvetlerine sağlanan eğitim olanakları, müşterek tatbikat ve alıştırmalar gözden geçirildi mi?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Siber olay müdahale planı güncel ve yeterli mi?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Siber olay müdahalesine ilişkin personel yeterliği teyit edildi mi?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Açıklama*			

f. Emniyet yönetimi

Emniyet düzenlemeleri ve önlemleri emniyet planına uygun mu?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Gizlilik derecesine sahip bilginin yetkisiz erişimden korunması amacıyla belirtilen doğrulamalar yapıldı mı?	1. Bilgi erişimine yetkilendirme	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	2. Bilgi bölümlendirme	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	3. Erişim kontrolü	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	4. Erişim prosedürleri	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	5. Belgelerin saklanması	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	6. Tespit etme	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
	7. Kayıt tutma ve işleme	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgisayarlarda ve bilgisayar tabanlı sistemlerde emniyet planına uygun seviyede koruma sağlandığı doğrulandı mı?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgisayarlarda ve bilgisayar tabanlı sistemlerde zafiyet analizleri yapıldı mı?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgisayarlarda ve bilgisayar tabanlı sistemler için gerçekleştirilen risk analizi güncel ve geçerli mi?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgi güvenliğine ilişkin düzenli farkındalık testleri ve değerlendirmeleri yapıldı mı?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgi güvenliği kapsamında verilerin yedeklemesi yapılmakta mı?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Bilgi güvenliği ve siber güvenlik dâhil emniyete ilişkin oluşturulan prosedürlerin düzenli olarak gözden geçirildiği ve güncellendiği doğrulandı mı?		<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır

Donanımın bakımı, test edilmesi ve sürdürülebilirliğine ilişkin kayıtlar gözden geçirildi mi?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Personelin güvenilirlik teyidinde ilişkin süreçlerin işlediği ve kayıt edildiği doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Özel güvenlik görevlilerinin ve emniyete ilişkin sorumluluğu bulunan diğer personelin gerekli yetkinliğe sahip olduğu doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Artan tehdit durumunda alınacak ek önlemler doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Emniyet personeli tarafından kullanılan talimat, kılavuz, yönerge gibi hususlarda yer alan bilgilerin güncelliği doğrulandı mı? (özel güvenlik görevlileri tarafından kullanılan talimatlarda yer alan iletişim numaralarının güncel olup olmadığının doğrulanması vb.)	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Açıklama*		

*İç denetim faaliyetlerine ilişkin bilgiler kapsamında neyin (erişim kontrolü, nükleer madde deposu vb.) nasıl denetlendiği (belge kontrolü, gözlem, test etme vb.) belirtilir. Ayrıca belirtmek istenen diğer hususlar da açıklanır.

2. Telafi Edici Önlemler

Tespit edilen bir bulgunun fiziksel koruma sisteminde önemli bir zafiyete yol açacağı değerlendirildiyse telafi edici önlemler alındı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Alınan telafi edici önlemin aynı ya da daha üst seviyede koruma seviyesi sağlayacağı doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Alınan telafi edici önlemin uzun vadeli düzeltici ve önleyici faaliyetler uygulanana kadar sürdürüleceği doğrulandı mı?	<input type="checkbox"/> Evet	<input type="checkbox"/> Hayır
Açıklama (iç denetim faaliyeti kapsamında bulgu tespit edilmesi durumunda alınacak telafi edici önlemlere ve bu önlemlerin fiziksel koruma sistemine etkisinin değerlendirilmesine ilişkin bilgiler verilir)		

3. İç Denetim Sonuçlarıyla İlgili Değerlendirme ve Öneriler

4. Emniyet Kapsamında Belirtilmek İstenen Diğer Detaylar

Tarih	Adı Soyadı		Ünvanı	İmza
	İç denetimi gerçekleştiren			
	İç denetimi onaylayan			