

DUYURU

Diyanet İşleri Başkanlığı Strateji Geliştirme Başkanlığında istihdam edilmek üzere; 375 Sayılı Kanun Hükmünde Kararname'nin Ek 6'ncı maddesi ile 31/12/2008 tarih ve 27097 sayılı Resmî Gazete'de yayımlanan Kamu Kurum ve Kuruluşlarının Büyük Ölçekli Bilgi İşlem Birimlerinde Sözleşmeli Bilişim Personeli İstihdamına İlişkin Esas ve Usuller Hakkında Yönetmelik'in 8'inci maddesi kapsamında sözlü/uygulamalı sınav başarı sırasına göre 10 adet sözleşmeli bilişim personeli alımı yapılacaktır.

MÜNHAL POSİZYONLARA AİT BİLGİLER				
BULUNDUĞU YER	BAŞVURU GRUBU	ÜNVAN	ADEDİ	AYLIK BRÜT SÖZLEŞME ÜCRETİ TAVAN KATSAYISI
Merkez Teşkilatı	A Grubu	Kıdemli Yazılım Geliştirme Uzmanı	2	3 Kata Kadar
	B Grubu	Yazılım Geliştirme Uzmanı	1	2 Kata Kadar
		DevOps Uzmanı	1	
		Sistem Uzmanı	1	
		Veri Tabanı Uzmanı	1	
		Mobil Uygulama Geliştirme Uzmanı	1	
		Siber Güvenlik Uzmanı	1	
		Sızma Testi Uzmanı	1	
		Bilgi Güvenliği Uzmanı	1	
	Toplam		10	

I. GENEL BAŞVURU ŞARTLARI

- 657 sayılı Devlet Memurları Kanunu'nun 48 inci maddesinin (A) bendindeki genel şartları taşımak,
- Fakültelerin dört yıllık bilgisayar mühendisliği, yazılım mühendisliği, elektrik mühendisliği, elektronik mühendisliği, elektrik ve elektronik mühendisliği ve endüstri mühendisliği bölümlerinden ya da bunlara denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yükseköğretim kurumlarından mezun olmak,
- 2 nci maddede belirtilenler dışında kalan dört yıllık eğitim veren fakültelerin mühendislik bölümlerinden, fen-edebiyat, eğitim ve eğitim bilimleri fakültelerinin, bilgisayar ve teknoloji üzerine eğitim veren bölümleri ile istatistik, matematik ve fizik bölümlerinden ya da bunlara denkliği Yükseköğretim Kurulunca kabul edilmiş yurt dışındaki yükseköğretim kurumlarından mezun olmak **(Bu kısımda belirtilen bölümlerden mezun olanlar brüt ücret tavanının 2 katı için başvuru yapabilirler.)**,
- Yazılım, yazılım tasarımı ve geliştirilmesi ile bu sürecin yönetimi konusunda veya büyük ölçekli ağ sistemlerinin kurulumu ve yönetimi konusunda ücret tavanı iki katını geçemeyecekler için en az 3 yıllık, diğerleri için ise en az 5 yıllık mesleki tecrübeye sahip bulunması **(Mesleki tecrübenin belirlenmesinde; bilişim personeli olarak 657 sayılı Kanuna tabi kadrolu veya aynı Kanunun**

4 üncü maddesinin (B) bendi ya da 399 sayılı Kanun Hükmünde Kararnameye tabi sözleşmeli statüdeki hizmetler ile özel kesimde sosyal güvenlik kurumlarına prim ödenmek suretiyle işçi statüsünde bilişim personeli olarak geçtiği belgelenen hizmet süreleri dikkate alınır).

5. Bilgisayar çevre birimlerinin donanımı ve kurulan ağ yönetimi güvenliği hakkında bilgi sahibi olmaları kaydıyla güncel programlama dillerinden en az ikisini bildiğini belgelemek,
6. Kamu Kurum ve Kuruluşlarının Büyük Ölçekli Bilgi İşlem Birimlerinde Sözleşmeli Bilişim Personeli İstihdamına İlişkin Esas ve Usuller Hakkında Yönetmelik'te yer alan özlük hakları ve diğer kuralları kabul etmek,
7. 2024 yılı KPSSP3 puan türünden en az 70 (yetmiş) puan almış olmak (**KPSS puanı olmayan yahut 70 (yetmiş) puandan az olan adayın KPSS puanı 70 (yetmiş) olarak dikkate alınacaktır.**),
8. İngilizce dilinde geçerliği devam eden Yabancı Dil Bilgisi Seviye Tespit Sınavı puanına veya Yükseköğretim Kurulunca bu dilde denkliği kabul edilen geçerli dil belgesine sahip olmak (**YDS puanına veya YÖK tarafından denkliği kabul edilen dil belgesine sahip olmayan adayların puanı 0 (sıfır) olarak dikkate alınacaktır.**).

- **Adaylar ilan edilen ünvanlardan sadece biri için başvuru yapabileceklerdir.**

II. ÖZEL BAŞVURU ŞARTLARI

A GRUBU

1. Kıdemli Yazılım Geliştirme Uzmanı (2 Kişi)

- a) Kamu kurumlarında veya büyük ölçekli özel sektör kuruluşlarında en az 5 (beş) yıl süreyle Kıdemli Yazılım Geliştirici ünvanıyla çalışmış olmak ve belgelemek,
- b) HTML, CSS, JavaScript gibi web teknolojileri ile en az 2 (iki) projede görev almış olmak,
- c) Yazılım geliştirme yaşam döngüsü, sürümleme ve dokümantasyon süreçlerine hakim olmak,
- d) .NET platformunda (C#, ASP.NET, .NET Core/.NET 6+) uygulama geliştirme konusunda ileri düzeyde bilgi ve deneyim sahibi olmak,
- e) Web servisleri ve API teknolojileri (REST, JSON, XML) ile çalışma konusunda tecrübeye sahip olmak,
- f) Yazılım mimarisi ve tasarım desenleri konusunda deneyim sahibi olmak (Örneğin:MVC, MVVM,DDD, CQRS gibi kavramlarla aktif olarak çalışmış olmak.),
- g) Kurumsal uygulamalarda mimari karar alma ve teknik rehberlik yapmış olmak (Özellikle yeni bir projenin teknik analiz ve yapılandırma aşamasında yer almış olmak.),
- h) Kod inceleme (code review), pull request değerlendirme süreçlerinde aktif rol almış olmak,
- i) RDBMS (MS SQL Server, PostgreSQL, MySQL vb.) veri tabanları ile uygulama geliştirmiş olmak ve ileri düzeyde SQL bilgisine sahip olmak,
- j) Versiyon kontrol sistemlerinden (Git, SVN vb.) en az birini aktif kullanmış olmak,
- k) Tercihen XSLT, XSD gibi XML teknolojilerinde bilgi sahibi olmak,
- l) Tercihen .NET uygulamalarında kimlik doğrulama ve yetkilendirme süreçlerinde (OAuth2, JWT, OpenID Connect) deneyim sahibi olmak,
- m) Tercihen birim testi, test otomasyonu ve hata ayıklama konularında bilgi sahibi olmak,
- n) Tercihen loglama ve izleme araçları konusunda deneyim sahibi olmak,
- o) Tercihen yazılım güvenliği konularında bilgi sahibi olmak,
- p) Tercihen Agile/Scrum gibi çevik yazılım geliştirme yöntemlerinde proje deneyimi sahibi olmak.

B GRUBU

2. Yazılım Geliştirme Uzmanı (1 Kişi)

- a) Kamu kurumlarında veya büyük ölçekli özel sektör kuruluşlarında yazılım geliştirme alanında en az 3 (üç) yıl mesleki tecrübeye sahip olmak ve belgelemek,
- b) Yazılım yaşam döngüsü, kod versiyonlama ve dokümantasyon süreçlerine hakim olmak ve XML işleme (XSLT, XSD) konusunda tecrübe sahibi olmak,
- c) Nesne yönelimli programlama (OOP) ve temel yazılım tasarım ilkeleri konusunda bilgi sahibi olmak,
- d) .NET platformunda (C#, ASP.NET, .NET Core) uygulama geliştirme konusunda bilgi sahibi olmak,
- e) Web tabanlı uygulamalar geliştirme konusunda tecrübeli olmak,
- f) RESTful servisler ve JSON/XML veri formatları ile çalışma konusunda deneyim sahibi olmak,
- g) RDBMS veritabanlarıyla (MS SQL Server, PostgreSQL, MySQL vb.) çalışmış olmak, temel SQL bilgisine sahip olmak,
- h) Versiyon kontrol sistemlerinden (Git, SVN vb.) en az birini aktif kullanmış olmak,
- i) Tercihen birim testleri ve hata ayıklama (debugging) konularında temel bilgi sahibi olmak,
- j) Tercihen yazılım güvenliği konusunda temel bilgilere sahip olmak,
- k) Takım çalışmasına yatkın, teknik dokümantasyon yapabilen ve iletişim becerileri güçlü olmak.

3. DevOps Uzmanı (1 Kişi)

- a) Uygulama sunucusu ve API yönetimi alanında toplamda en az 3 (üç) yıl tecrübe sahibi olmak ve belgelemek,
- b) Dağıtık sistem mimarileri, servis tabanlı yapı (SOA) ve mikroservis mimarisi hakkında temel bilgiye sahip olmak,
- c) Sistem yönetimi, ağ yapıları, servis güvenliği ve erişim kontrolü konularında bilgi sahibi olmak,
- d) Uygulama sunucu kurulumu, yapılandırılması, deploy, log analizi ve sorun giderme süreçlerinde deneyimli olmak,
- e) Web sunucularının yapılandırması ve yönlendirme ayarları (reverse proxy, SSL termination vb.) konularında bilgi sahibi olmak,
- f) API Gateway platformlarından en az biriyle uygulamalı deneyime sahip olmak,
- g) API'lerin yayınlanması (publish), versiyonlanması, rate limiting, throttling, authentication (OAuth2, JWT), IP whitelisting ve CORS yönetimi gibi gateway politikalarını uygulayabilmek,
- h) API anahtarı (API key), access token, güvenli API çağrıları ve kullanıcı kimlik doğrulama mekanizmalarını yönetebilmek,
- i) Uygulama ve API erişim loglarını yorumlayabilmek, performans ve güvenlik için izleme çözümleri ile çalışmış olmak (Prometheus, Grafana, ELK vb.),
- j) Linux/Unix ortamlarında uygulama kurulumları, betik yazımı (Bash, Shell), log takibi ve sistem ayarları konusunda bilgi sahibi olmak,
- k) Tercihen Docker/Kubernetes gibi konteyner teknolojileriyle uygulama ve API yönetimi deneyimi olmak,
- l) Tercihen kimlik ve erişim yönetimi (SSO, LDAP, OAuth2) altyapılarıyla entegrasyon tecrübesine sahip olmak,
- m) Tercihen güvenlik duvarı, SSL sertifikaları, TLS yapılandırmaları ve güvenli API tasarımı konularında bilgi sahibi olmak,
- n) Tercihen CI/CD süreçlerine aşinalık (Jenkins, GitLab CI, Ansible vb.) ve deployment otomasyonu bilgisi olmak,
- o) Tercihen ITIL, ISO/IEC 27001 gibi standartlara uygunluk konusunda çalışmış olmak veya bilgi sahibi olmak,
- p) Tercihen API yaşam döngüsü yönetimi (API lifecycle management), gateway clustering ve yüksek erişilebilirlik çözümlerinde görev almış olmak,
- q) Takım çalışmasına yatkın, analitik düşünen, teknik dokümantasyon yapabilen ve sistematik çalışma alışkanlığına sahip olmak.

4. Sistem Uzmanı (1 Kişi)

- a) Uygulama sunucusu ve API yönetimi alanında toplamda en az 3 (üç) yıl tecrübe sahibi olmak ve belgelemek,
- b) Temel ağ teknolojileri, TCP/IP, DNS, DHCP, NAT, VLAN, VPN, Load Balancer gibi kavramlara hakim olmak,
- c) Sunucu, işletim sistemi ve sistem güvenliği konularında bilgi sahibi olmak,
- d) Windows Server (2016 ve üzeri) ve/veya Linux tabanlı (Red Hat, CentOS, Ubuntu vb.) sunucu işletim sistemlerinin kurulumu, yapılandırılması, yedekleme ve izleme işlemlerinde deneyim sahibi olmak,
- e) Group Policy, DNS, DHCP, File Server gibi servislerin kurulumu, yönetimi ve sorun giderme süreçlerinde bilgi sahibi olmak,
- f) Sanallaştırma platformlarından (VMware vSphere/ESXi, Proxmox vb.) en az birinde deneyim sahibi olmak,
- g) Linux ve Windows sistemlerde güvenlik açıklarını analiz edebilmek ve istismar (exploit) edebilmek,
- h) Yedekleme ve felaket kurtarma (Disaster Recovery) çözümleri konusunda bilgi sahibi olmak,
- i) Merkezi loglama, izleme ve alarm sistemleri (Zabbix, Nagios, ELK, Grafana vb.) hakkında bilgi sahibi olmak,
- j) Temel düzeyde komut satırı ve betik dili bilgisi (PowerShell ve/veya Bash) sahibi olmak,
- k) Tercihen yüksek erişilebilirlik (HA), yük dengeleme (Load Balancing) ve cluster sistemleri hakkında bilgi sahibi olmak,
- l) Tercihen merkezi kimlik doğrulama sistemleri (LDAP, RADIUS, SSO, MFA) konusunda tecrübe sahibi olmak,
- m) Tercihen kamu kurumlarında veya kullanıcı sayısı yüksek ortamlarda sistem yönetimi tecrübesine sahip olmak,
- n) Takım çalışmasına yatkın, kriz anlarında çözüm odaklı hareket edebilen ve teknik dokümantasyon yapabilen bir yapıya sahip olmak,
- o) ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi hakkında bilgi sahibi olmak, bilgi güvenliği politikalarına uygun sistem yönetimi gerçekleştirebilecek bilgiye sahip olmak,
- p) ITIL servis yönetim süreçleri (Incident, Change, Problem Management vb.) hakkında bilgi sahibi olmak ve bu süreçlere uygun şekilde teknik destek verebilecek bilgiye sahip olmak.

5. Veri Tabanı Uzmanı (1 Kişi)

- a) Veri tabanı yönetimi alanında en az 3 (üç) yıl tecrübeye sahip olmak ve belgelemek,
- b) Oracle Certified Professional (OCP), Microsoft Certified: Azure Database Administrator Associate, PostgreSQL Certified Professional, MySQL Database Administrator Certified Professional sertifikalarından en az bir tanesine sahip olmak veya bunlara eşdeğer uluslararası geçerliliğe sahip veri tabanı yönetimi sertifikalarından birine sahip olmak ve belgelendirmek,
- c) Veri tabanı yönetimi, yedekleme, performans iyileştirme ve güvenliği alanlarında çalıştığını gösterir SGK hizmet dökümü veya çalıştığı kurumdaki alınmış referans yazısını belgelendirmek,
- d) DBMS mimarisi hakkında bilgi sahibi olmak ve en az bir ilişkisel veri tabanı yönetim sisteminde (MS SQL Server, PostgreSQL, MySQL vb.) aktif olarak çalışmış olmak,
- e) Veri güvenliği, veri bütünlüğü ve yedekleme konularında bilgi sahibi olmak,
- f) Microsoft SQL Server, PostgreSQL veya MySQL gibi yaygın veri tabanı sistemlerinden en az birinde ileri düzeyde yönetim bilgisine sahip olmak (kullanıcı, yetki, şema, indeks, trigger, view, stored procedure, function vb. konular),
- g) Performans izleme, sorgu optimizasyonu (query tuning), indeksleme ve kaynak yönetimi konularında deneyimli olmak,
- h) Veri yedekleme, kurtarma ve felaket senaryolarının uygulanması konularında bilgi sahibi olmak (pg_dump, SQL Server Backup vb.),

- i) Yüksek erişilebilirlik çözümleri konusunda bilgi sahibi olmak (Always On, Log Shipping, Replication, Cluster, Streaming Replication vb.),
- j) Veri aktarımı, dışa/içe veri yükleme (import/export), ETL işlemleri ve veri taşıma süreçlerinde görev almış olmak,
- k) Tercihen veri maskeleyme, anonimleştirme, loglama ve audit süreçleri konusunda bilgi sahibi olmak,
- l) Tercihen kurumsal ölçekte, büyük hacimli veri yapıları üzerinde çalışmış olmak,
- m) Tercihen veri tabanı izleme ve yönetim araçlarını kullanmış olmak (OEM, SQL Server Management Studio, pgAdmin, DBeaver, Zabbix entegrasyonu vb.),
- n) Tercihen ITIL süreçlerine aşinalık ve 27001 Bilgi Güvenliği Yönetim Sistemi çerçevesinde veri tabanı yönetimi tecrübesi,
- o) Takım çalışmasına yatkın olmak, düzenli teknik dokümantasyon hazırlayabilmek ve güvenlik politikalarına uygun çalışabilmek.

6. Mobil Uygulama Geliştirme Uzmanı (1 Kişi)

- a) Mobil uygulama geliştirme alanında en az 3 (üç) yıl tecrübeye sahip olmak ve belgelemek,
- b) Yazılım geliştirme yaşam döngüsüne, kod versiyonlama süreçlerine ve temel yazılım mimarilerine hakim olmak,
- c) Uygulama güvenliği, veri gizliliği ve mobil platformlara özgü kısıtlar konusunda bilgi sahibi olmak,
- d) Android (Java/Kotlin) ve/veya iOS (Swift/Objective-C) platformlarında mobil uygulama geliştirme konusunda uygulamalı tecrübe sahibi olmak,
- e) Tercihen Flutter, React Native, gibi çapraz platform teknolojilerinden en az biriyle uygulama geliştirmiş olmak,
- f) RESTful API servisleri ile mobil uygulama entegrasyonu konusunda bilgi sahibi olmak,
- g) JSON, XML gibi veri formatlarıyla çalışabilecek bilgiye sahip olmak,
- h) Mobil uygulamalarda performans optimizasyonu, bellek yönetimi ve hata ayıklama (debugging) konularında tecrübeli olmak,
- i) Uygulama mağazalarına (Google Play, Apple App Store) yükleme, sürüm güncelleme ve dağıtım süreçlerine hakim olmak,
- j) Git veya benzeri bir versiyon kontrol sistemi ile çalışmış olmak,
- k) Mobil uygulamalarda bildirim sistemleri (push notification), kamera, harita, dosya sistemi vb. cihaz donanımlarına erişim konularında bilgi sahibi olmak,
- l) Tercihen kullanıcı dostu arayüz (UI) ve kullanıcı deneyimi (UX) tasarım ilkelerine uygun uygulama geliştirmiş olmak,
- m) Tercihen mobil uygulamalarda kimlik doğrulama ve güvenlik uygulamaları (JWT, OAuth2, biometric authentication) hakkında bilgi sahibi olmak,
- n) Tercihen Firebase, Google Maps, App Center gibi servisleri mobil uygulamalarda entegre olarak kullanmış olmak,
- o) Tercihen mobil uygulama test araçları (Appium, Espresso, XCTest vb.) ve otomasyon süreçleri hakkında bilgi sahibi olmak.

7. Siber Güvenlik Uzmanı (1 Kişi)

- a) Ağ sistemleri ve/veya bilgi güvenliği alanında en az 3 (üç) yıl tecrübeye sahip olmak ve belgelemek,
- b) Temel ağ teknolojileri, protokoller ve mimariler konusunda bilgi sahibi olmak (TCP/IP, UDP, VLAN, NAT, Routing, Switching vb.),
- c) Bilgi güvenliği yönetimi, erişim kontrolü, güvenlik politikaları ve risk değerlendirme konularında bilgi sahibi olmak,
- d) Firewall, IPS/IDS, VPN, Proxy, WAF gibi ağ güvenlik cihazları ve sistemlerinin kurulumu, yapılandırılması ve yönetimi konusunda deneyimli olmak,
- e) Windows ve Linux sistemlerde güvenlik açıklarının tespiti ve temel sertifika yönetimi konularında bilgi sahibi olmak,

- f) Güvenlik duvarı kuralları, port güvenliği, ağ segmentasyonu ve DMZ yapılandırmaları konularında deneyim sahibi olmak,
- g) Antivirüs, EDR/XDR çözümleri gibi uç nokta ve ağ güvenliği ürünlerinde deneyim sahibi olmak,
- h) Penetrasyon testi ve zafiyet tarama araçları (Nessus, Nmap, OpenVAS, Metasploit vb.) hakkında bilgi sahibi olmak,
- i) Tercihen ISO/IEC 27001, KVKK, NIST gibi standartlara uygun güvenlik test süreçlerine katkı sağlamış olmak,
- j) Tercihen ITIL süreçlerine aşinalık (özellikle Incident, Change ve Problem Management),
- k) Tercihen kamu kurumlarında ya da yüksek güvenlik gerektiren ortamlarda görev almış olmak,
- l) Tercihen SIEM sistemleri ile log toplama, analiz ve korelasyon işlemleri gerçekleştirebilmek,
- m) Takım çalışmasına yatkın olmak, stres altında çalışabilmek, teknik dokümantasyon ve raporlama yapabilmek.

8. Sızma Testi Uzmanı (1 Kişi)

- a) Bilgi güvenliği, sızma testleri veya güvenlik denetimi alanında en az 3 (üç) yıl tecrübeye sahip olmak ve belgelendirmek,
- b) CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional) veya TSE onaylı Sızma Testi Sertifikasına sahip olmak veya bunlara eşdeğer uluslararası geçerliliğe sahip sızma testi sertifikalarından birine sahip olmak ve belgelendirmek,
- c) Sızma testi alanında çalıştığını gösterir SGK hizmet dökümü veya çalıştığı kurumdan alınmış referans yazısını belgelendirmek,
- d) Bilgi güvenliği temelleri, güvenlik açıkları, tehdit vektörleri, protokol zafiyetleri ve güvenlik mimarileri hakkında bilgi sahibi olmak,
- e) İç ve dış ağ sızma testleri, web uygulama testleri, mobil uygulama testleri ve kablosuz ağ testleri konularında pratik deneyime sahip olmak,
- f) Penetrasyon testi araçlarına hâkim olmak (Nmap, Metasploit, Burp Suite, Nessus, Nikto, sqlmap, Hydra, John the Ripper, Wireshark vb.),
- g) Zafiyet tarama, exploit geliştirme, privilege escalation, password cracking gibi alanlarda uygulamalı bilgi sahibi olmak,
- h) Web uygulama güvenliği testlerinde kullanılan manuel tekniklere ve otomatik araçlara hakim olmak,
- i) Linux ve Windows sistemlerde güvenlik açıklarını analiz edebilmek ve istismar (exploit) edebilmek,
- j) Raporlama konusunda yetkin olmak; test sonuçlarını teknik ve yönetsel düzeyde açıklayabilen raporlar hazırlayabilmek,
- k) Tercihen TSE onaylı "Sızma Testi Sertifikası"na sahip olmak veya TSE'nin yetkilendirdiği bir kuruluşta sızma testi gerçekleştirmiş olmak,
- l) Tercihen OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), eJPT, GPEN gibi uluslararası geçerliliğe sahip sertifikalardan bir veya birkaçına sahip olmak,
- m) Tercihen SIEM, DLP, EDR/XDR, IDS/IPS sistemleriyle entegre çalışan güvenlik ortamlarında test gerçekleştirmiş olmak,
- n) Tercihen kaynak kod analizi, güvenli yazılım geliştirme süreçleri ve uygulama güvenliği testleri hakkında bilgi sahibi olmak,
- o) Tercihen ISO/IEC 27001, KVKK, NIST gibi standartlara uygun güvenlik test süreçlerine katkı sağlamış olmak.

9. Bilgi Güvenliği Uzmanı (1 Kişi)

- a) Bilgi güvenliği, siber güvenlik, risk yönetimi veya denetim alanında en az 3 (üç) yıl tecrübeye sahip olmak ve belgelemek,
- b) Bilgi güvenliği standartları, politikaları, süreç yönetimi ve güvenlik mimarileri hakkında bilgi sahibi olmak,
- c) ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı ve uygulamaları konusunda bilgi ve deneyim sahibi olmak,
- d) KVKK, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5651 sayılı yasa, Bilgi Güvenliği Rehberi, TSE, NIST, COBIT gibi ulusal ve uluslararası düzenlemelere aşinalık ve bu kapsamlarda uyumluluk çalışmalarında görev almış olmak,
- e) Kurumsal risk analizleri gerçekleştirebilmek, risk değerlendirme ve risk işleme planları hazırlayabilmek,
- f) Bilgi güvenliği politikaları, prosedürleri, talimatları ve farkındalık çalışmalarının hazırlanması ve uygulanması süreçlerinde görev almış olmak,
- g) İç denetim, dış denetim ve sertifikasyon süreçlerinde bilgi güvenliği tarafında destek vermiş olmak,
- h) Güvenlik ihlali, olay müdahalesi (incident response), veri sızıntısı tespiti ve raporlama süreçlerine katkı sağlayabilecek bilgi ve beceriye sahip olmak,
- i) Tercihen ISO/IEC 27001 İç Denetçi, ISO 27005 Risk Yönetimi, ISO 22301 İş Sürekliliği gibi sertifikalardan en az birine sahip olmak,
- j) Tercihen bilgi güvenliği denetimi ve uyum kontrollerinde aktif görev almış olmak,
- k) Tercihen güvenlik açığı yönetimi, zafiyet tarama, sızma testi çıktılarının analiz edilmesi ve riskle ilişkilendirilmesi konularında bilgi sahibi olmak,
- l) Tercihen bilgi güvenliği farkındalık eğitimleri, kullanıcı bilgilendirme çalışmaları ve sosyal mühendislik testlerinde rol almış olmak,
- m) Tercihen ITIL ve ISO 20000 gibi hizmet yönetim standartları hakkında temel bilgi sahibi olmak,
- n) Takım çalışmasına yatkın, analitik düşünce yapısına sahip, güçlü yazılı ve sözlü iletişim becerisi olan, dokümantasyon konusunda disiplinli çalışabilmek.

III. İSTENİLEN BELGELER

1. Adaylar Genel Başvuru Şartları ile her bir pozisyon için belirlenmiş olan “Özel Başvuru Şartları” başlığında istenilen sertifikalar ile mesleki tecrübe veya deneyimi gösteren belgeleri başvuru ekranında yer alan ilgili bölüme yükleyeceklerdir.
2. Başvurulan pozisyon için mesleki tecrübe şartını gösteren belgelerin; (başvurulan pozisyon ile ilgili alan bilgisi, çalışılan hizmetler/projeler ve bu hizmetlerin/projelerin kapsamı, çalışma süreleri vb.) **pdf** veya **jpeg** formatında yüklenmesi gerekmektedir. Adaylardan gerekli durumlarda sisteme yüklenen belgelerin asılları istenilebilecektir.
3. Özel Başvuru Şartları başlığında belgelenmesi istenilen niteliklerin ibraz edilen belgede yer almaması ya da tam olarak anlaşılmaması durumunda başvurular geçersiz sayılacaktır.

IV. BAŞVURU İŞLEMLERİ

1. Müracaatlar, başvuru şartlarını taşıyan adayların bizzat kendileri tarafından 02.02.2026–20.02.2026 (saat 16:30) tarihleri arasında DİBBYS programı üzerinden [“sinav.diyinet.gov.tr”](https://sinav.diyinet.gov.tr) adresi aracılığı ile yapılacaktır.
2. Adayların öğrenim durumları elektronik ortamda tespit edilecektir. Öğrenim bilgileri elektronik ortamda bulunmayan adaylar, başvuru işlemlerinden önce mezuniyet bilgilerini ilgili kurumlar (üniversiteler) aracılığıyla elektronik ortama kaydettireceklerdir.
3. Adaylar Genel Başvuru Şartları ile Özel Başvuru Şartları başlığı altında istenilen belgeyi başvuru ekranındaki ilgili bölüme PDF veya JPEG formatında yükleyeceklerdir.
4. Adaylar, başvuru ekranındaki ilgili alana iş deneyimini gösteren 1000 karakteri aşmayacak şekilde öz geçmişlerini yazacaklardır.
5. Başvuru işlemlerinin hatasız, eksiksiz ve duyuruda belirtilen hususlara uygun olarak yapılmasından adayların kendileri sorumlu olacaktır.

6. Müracaatların sona ermesinden sonra adayın başvuru bilgilerinde hangi nedenle olursa olsun kesinlikle değişiklik yapılmayacaktır.
7. Bu duyuruda belirlenen esaslara uygun olmayan başvurular kabul edilmeyecektir.

V. SINAVA İLİŞKİN TEBLİGAT VE DUYURULAR

1. Sınav ve sonuçları ile ilgili bütün duyurular Başkanlığımız internet sitesinde ve aynı sitedeki İnsan Kaynakları Genel Müdürlüğü sayfasında ilan edilecektir. Adaylara ayrıca tebligat yapılmayacaktır.
2. Sınav Giriş Belgesi alma ve sınav sonuç öğrenme işlemleri adaylar tarafından "sinav.diyagnet.gov.tr" adresi aracılığıyla gerçekleştirilecektir.

VI. SINAVA ÇAĞIRMA, SINAVIN YERİ VE TARİHİ

1. Sınav sözlü/uygulamalı olarak 03.03.2026 tarihinde Ankara'da başlatılacaktır.
2. 2024 yılı lisans düzeyi Kamu Personel Seçme Sınavı (KPSS) P3 puanının yüzde yetmişi ile yabancı dil puanının yüzde otuzunun toplamı esas alınarak başvurular arasından en yüksek puana sahip adaydan başlamak suretiyle atama yapılacak kadro sayısının 10 (on) katı aday, son sıradaki adayla aynı puanı alanlar dahil olmak üzere sınava çağrılacaktır.
3. Adaylar sınava gelirken "Sınav Giriş Belgesi" ile birlikte kimlik belgesini (nüfus cüzdanı, kimlik kartı veya pasaport) yanlarında bulunduracaklardır. Kimlik belgesi ile sınav giriş belgesi bulunmayan adaylar sınava alınmayacaktır. Nüfus cüzdanı, kimlik kartı veya pasaport dışında başka bir belge kimlik belgesi olarak kabul edilmeyecektir.

VII. SINAV SONUÇLARINA İTİRAZ

1. Adaylar tarafından sözlü sınav sonuçlarına ilişkin itirazlar sözlü/uygulamalı sınavın sonuçlarının ilan edilmesinden itibaren 5 (beş) gün içinde duyuruda belirtilen "Yazışma Adresi"ne yapılacaktır. Belirtilen süre içerisinde ulaştırılmayan ve "DİĞER HUSUSLAR" başlığında belirtilen şekilde yapılmayan itirazlar dikkate alınmayacaktır.
2. İtirazların sonucu, yapılan inceleme neticesinde ilgililere yazılı olarak bildirilecektir.
3. Süresi içinde yapılmayan itirazlar işleme alınmayacaktır.

VIII. DEĞERLENDİRME VE BAŞARI SIRALAMASI

1. Sınavda başarılı olabilmek için sözlü/uygulamalı sınavdan 100 (yüz) tam puan üzerinden en az 70 (yetmiş) puan almak gerekmektedir.
2. Başarılı olanlardan ilan edilen pozisyon sayısı kadarı asıl, ilan edilen pozisyon sayısı kadar aday da yedek olarak sıralanacaktır.

IX. DİĞER HUSUSLAR

1. **7315 Sayılı Güvenlik Soruşturması ve Arşiv Araştırması Kanunu gereğince güvenlik soruşturması/arşiv araştırması sonucu olumlu olan adayların ataması yapılacaktır.**
2. Başkanlık, sınav sürecinin her aşamasında adaylar tarafından belirtilen hususlarda adaylardan ayrıca bilgi ve belge talep edebilecektir.
3. Sınav öncesi, sonrası ve yerleştirme sürecindeki işlemlerde gerçeğe aykırı belge verdiği ya da beyanda bulunduğu tespit edilen adayların başvuru ve sınavları geçersiz sayılacaktır.
4. Adayların, sınavın tüm aşamalarıyla ilgili taleplerini T.C. kimlik numarası, adı, soyadı, imza ve adreslerinin yer aldığı ıslak imzalı yazılı dilekçe ile Başkanlığımız İnsan Kaynakları Genel Müdürlüğü Personel Sistemleri Eğitim ve Sınavlar Daire Başkanlığına ulaştırmaları gerekmektedir. Faks ve e-posta ile ulaştırılan talepler dikkate alınmayacaktır.
5. Bu duyuruda yer almayan hususlarla ilgili olarak 657 sayılı Devlet Memurları Kanunu, 375 sayılı Kanun Hükmünde Kararname, Kamu Kurum ve Kuruluşlarının Büyük Ölçekli Bilgi İşlem Birimlerinde Sözleşmeli Bilişim Personeli İstihdamına İlişkin Esas ve Usuller Hakkında Yönetmelik hükümleri geçerlidir.

X. İLETİŞİM

Yazışma Adresi : Diyanet İşleri Başkanlığı İnsan Kaynakları Genel Müdürlüğü
Personel Sistemleri Eğitim ve Sınavlar Daire Başkanlığı
Üniversiteler Mah. Dumlupınar Blv. No:147/A 06800 Çankaya/ANKARA
Telefon : (0312) 295 77 63
E-posta : persis@diyanet.gov.tr

İlgililere duyurulur.

DİYANET İŞLERİ BAŞKANLIĞI
İNSAN KAYNAKLARI GENEL MÜDÜRLÜĞÜ