BGYS POLİTİKASI

Politika Numarası	PLTK-23
Politika Tanımı	Kaynak Kodlara Erişim Politikası
Amaç ve İlkeler	**Bu politika,** Kayalar Şirketi'nin bilgi varlıkları arasında yer alan kaynak kodlarına erişimi yönetmek için oluşturulmuştur. Ayrıca, bilgi güvenliği ve gizliliğini sağlamak amacıyla belirlenen kuralları ve prosedürleri içerir.
Sorumluluklar	**Bilgi İşlem Personeli:** Politika dışı davranılmasının engellenmesi amacıyla sistem kurulması ve kurulan sistemin denetlenmesinden sorumludur. **Tüm çalışanlar:** Belirlenen politika ve prosedürlere uymakla yükümlüdür.
Sapma ve Özel Durumlar	Sapmalar veya özel durumlarla karşılaşıldığında, ilgili departman veya yöneticilerle iletişime geçilmelidir. Bu durumlar, politikanın etkinliğini artırmak için incelenir ve gerekli düzeltici önlemler alınarak, uygun cezai yaptırımlar gerçekleştirilir.

UYGULAMA

- Kaynak kodlarına ve kütüphanelere erişim, iş gereksinimlerine dayalı olarak belirlenen yetkilendirme doğrultusunda yapılmalıdır.
- İş rolleri, projeler ve diğer kriterler göz önünde bulundurularak erişim yetkilendirmesi yapılmalıdır.
- Yeni çalışanlar için erişim yetkilendirmesi, İnsan Kaynakları Departmanı ve Bilgi İşlem Birimi tarafından belirlenen şartlar dahilinde gerçekleştirilmelidir.
- İzinler, kullanıcıların belirli kaynak kodlarını okuma, yazma veya sadece görüntüleme yetkisini içermelidir.
- Mevcut çalışanların erişim yetkilendirmesi, güncel iş gereksinimleri göz önünde bulundurularak düzenli olarak gözden geçirilir ve gerektiğinde güncellenmelidir.
- Erişim seviyeleri ve izinler, kullanıcıların belirli kaynak kodlarını ve kütüphaneleri okuma, yazma veya sadece görüntüleme yetkilerini belirler.
- Kısıtlamalar, belirli kullanıcıların belirli kaynak kodlarına veya kütüphanelere erişimini sınırlar veya engeller.

İş gereksinimlerine dayalı olarak kaynak koduna okuma ve yazma erişimi onayı verilmesi, kötüye kullanma risklerinin engellenmesi amacıyla;

- İş birimleri, projeler veya görevler için gerekli olan erişim yetkilendirmesi, ilgili yöneticiler tarafından onaylanmalı ve Bilgi İşlem Birimi tarafından uygulanmalıdır.
- Erişim yetkilendirmesi verilirken, değişiklik veya kötüye kullanma risklerinin değerlendirilmesi önemlidir. Bilgi İşlem Birimi, her erişim yetkilendirmesi talebi için risk analizi yapmalı ve olası riskleri belirlemelidir. Değişiklik veya kötüye kullanma riskleri belirlendikten sonra, uygun önlemler alınarak bu riskler yönetilip ve azaltılmalıdır.
- Erişim yetkilendirmeleri sonrasında, kaynak kodu ve yazma erişimi kullanıcılarının faaliyetleri düzenli olarak izlenip ve denetlenmelidir. İzleme ve denetleme süreçleri, erişim politikalarının uygun şekilde uygulandığını ve işlendiğini sağlamaktadır.
- Herhangi bir anormallik veya güvenlik ihlali tespit edildiğinde, derhal müdahale edilip gerekli düzeltici eylemler alınmalıdır.
- Politika ve prosedürler düzenli olarak gözden geçirilip güncellenmelidir. Yapılan değişiklikler, bilgi güvenliği risklerine yanıt olarak veya iş gereksinimlerine uyum sağlamak için yapılır.
- İyileştirme süreci, şirketin bilgi güvenliği ve iş sürekliliği hedeflerine daha iyi ulaşmak için devamlı olarak değerlendirilmelidir.

Bu uygulamalar, firmamızın iş gereksinimlerine dayalı kaynak kodu erişimi ve risk yönetimi konusundaki taahhüdünü yansıtmaktadır.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
02.02.2024	-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı

BGYS POLİTİKASI

Kaynak kodunun ve ilişkili unsurların güncellenmesi ve değişiklik kontrol işlemlerine uygun olarak kaynak koduna erişim izni verilmesi ve yalnızca uygun yetki alındıktan sonra gerçekleştirilmesi konusuna dikkat edilmelidir. Güvenlik ve denetim amacıyla kaynak kodunun güvenliği ve bütünlüğünü korumak amacıyla kod deposuna doğrudan erişim verilmemesi yaklaşımı benimsenmelidir. Erişim izinleri, geliştirici araçları aracılığıyla kontrol edilip yönetilmelidir.

Geliştirici araçlarına erişim izni talepleri, ilgili proje yöneticileri veya departman yöneticileri tarafından incelenmelidir. Erişim talepleri, proje gereksinimleri ve güvenlik politikaları doğrultusunda değerlendirilip uygun yetkilerle sınırlı olarak onaylanmalıdır.

Geliştirici araçları üzerinden sağlanan erişimler, belirli yetkilerle sınırlı olup, gereksiz erişimler engellenmelidir. Erişim izinleri ve etkinlikleri düzenli olarak izlenip gereksiz erişimler tespit edilmelidir.

Geliştirici araçlarındaki yetki ve erişimler periyodik olarak gözden geçirilip gerektiğinde revize edilmelidir. Personel değişiklikleri veya proje gereksinimleri gibi durumlarda yetki revizyonları yapılıp uygun şekilde yönetilmelidir.

Bu yaklaşım sayesinde, kaynak kodunun güvenliği ve bütünlüğü sağlanırken, geliştiricilere gereksinim duydukları yetkiler ve erişimler kontrollü bir şekilde sağlanmaktadır.

Program listelerininin, okuma ve yazma erişiminin uygun şekilde yönetilmesi ve atanması gereken güvenli bir ortamda tutulması amacıyla;

- Program listelerine erişim izinleri, ilgili departman yöneticileri veya yetkilendirilmiş personel tarafından yapılmalıdır. Erişim izinleri, iş gereksinimleri ve güvenlik politikaları doğrultusunda belirlenip yönetilmelidir.
- Program listelerindeki verileri okuma ve yazma erişimi, sadece yetkilendirilmiş personel tarafından sağlanmalıdır. Erişim izinleri, belirli yetkilerle sınırlı olarak atanır ve gereksiz erişimler engellenir.
- Program listeleri, güvenli bir ortamda tutulup yetkisiz erişimlerden korunmalıdır. Fiziksel güvenlik önlemleri ve dijital güvenlik önlemleri, program listelerinin güvenliğini sağlamak için uygulanmalıdır.
- Program listelerine erişimler düzenli olarak izlenip denetlenmelidir. Erişim kayıtları tutulmalı ve gerektiğinde incelenmelidir. Herhangi bir anormallik veya güvenlik ihlali durumunda, derhal müdahale edilip gereken düzeltici önlemler alınmalıdır.
- Personel, program listelerinin güvenliği konusunda düzenli eğitim ve farkındalık programlarıyla bilgilendirilmelidir. Bilinçli kullanıcılar, güvenlik önlemlerinin etkin bir şekilde uygulanmasına katkıda bulunur.

Tüm erişimlerin ve kaynak koddaki tüm değişikliklerin bir denetim günlüğünün (loglarının) tutulması amacıyla;

- **Erişim Denetim Günlüğü:** Sistemlerde, özellikle kaynak kod deposunda, kimin sisteme eriştiğini ve hangi dosyaların erişildiğini kaydeden günlüklerdir.
- **Değişiklik Denetim Günlüğü:** Kaynak kodunda yapılan her değişiklik, kimin ne zaman ve neyi değiştirdiğini belirten bir günlükte kaydedilir.

Günlükler, güvenli bir şekilde saklanıp yasal gereksinimlere uygun olarak belirlenen bir süre boyunca korunmalıdır.

Günlükler düzenli olarak izlenip denetlenmelidir. Güvenlik ihlalleri tespit edilirse, hızlı müdahale edilip gerekli önlemler alınmalıdır.

YAYIMLANMA TARİHİ	REVİZYON NO/TARİHİ	HAZIRLAYAN	ONAYLAYAN
02.02.2024	-	Mehmet YALÇIN BGYS Temsilcisi	Yusuf KAYA Genel Müdür Yardımcısı