BGYS POLİTİKASI

Politika Numarası	PLTK-21
Politika Tanımı	Çıkarılabilir Depolama Ortamı Yönetimi Politikası
Amaç ve İlkeler	**Bu politika,** Kayalar Şirketi'nde kullanılan taşınabilir depolama cihazlarının (USB sürücüler, harici diskler vb.) güvenliğini sağlamak, veri bütünlüğünü korumak ve güvenli veri aktarımını teşvik etmek için yapılmıştır.
Sorumluluklar	**Bilgi İşlem Personeli:** Sistem kurma ve denetleme gibi teknik sorumlulukları üstlenirler. Bu ekip, taşınabilir depolama cihazlarının güvenliğini sağlamakla görevlidir. **Tüm Çalışanlar:** Politika ve prosedürlere uymakla yükümlüdürler. Çalışanlar, taşınabilir depolama cihazlarını güvenli bir şekilde kullanmayı ve politikaları anlamayı sağlamalıdır.
Sapma ve Özel Durumlar	Politika dışı davranışlar veya özel durumlarla karşılaşıldığında, çalışanlar durumu derhal ilgili departman veya yöneticilere bildirmelidir. Bu durumlar incelenecek, gerekli düzeltici önlemler alınacak ve uygun cezai yaptırımlar uygulanacaktır.

UYGULAMA

Çıkarılabilir depolama ortamı, bilgisayar veya diğer elektronik cihazlara veri depolamak ve transfer etmek amacıyla kullanılan, kolaylıkla takılıp çıkarılabilen taşınabilir depolama cihazlarıdır.

Tüm depolama ortamlarındaki veriler, hassasiyet düzeylerine göre sınıflandırılmalıdır. Sınıflandırma, verilerin gizliliği, bütünlüğü ve erişilebilirliği gözetilerek yapılmalıdır.

Bilgi sınıflandırmasına göre belirlenen veri hassasiyet düzeylerine uygun olarak, özel güvenlik önlemleri alınmış depolama alanları oluşturulmalıdır. Bu alanlar, sadece belirli yetkilendirilmiş personelin erişebileceği biyometrik güvenlik sistemleri ile korunmalıdır.

Depolama alanları, ısı, nem, rutubet ve elektronik alan gibi çevresel tehditlere karşı imalatçı spesifikasyonlarına uygun olarak tasarlanmalıdır. Sıcaklık ve nem seviyeleri sürekli olarak izlenir ve gerektiğinde otomatik sistemlerle düzeltilir.

Depolama ortamlarındaki elektronik ekipmanlar, elektromanyetik alanlardan etkilenmemesi için özel kabinler içerisinde korunmalıdır. Bu kabinler, elektromanyetik koruma sağlayarak hassas cihazların güvenli bir şekilde depolanmasını sağlamaktadır.

Depolama alanları, güvenlik kameraları ve giriş/çıkış noktalarındaki güvenlik personeli ile 24/7 izlenir ve korunmalıdır. Fiziksel güvenlik kontrolleri, sadece yetkilendirilmiş personelin belirli alanlara erişimine izin verir. Tüm depolama ortamları, imalatçıların belirttiği periyodik bakım ve güvenlik kontrollerine tabi tutulmalıdır. Elektronik ekipmanlar için belirlenen ömürleri boyunca düzenli olarak güncellenip ve yenilenmelidir.

Çalışanlar, depolama ortamlarının güvenliği konusunda eğitilir ve düzenli olarak bilinçlendirme programlarına katılır.

Bilgilerin gizliliği, bütünlüğü ve erişilebilirliği konularında özellikle çıkarılabilir depolama ortamlarındaki bilgilerin güvenliğini sağlamak adına kriptografik tekniklerin etkin bir şekilde kullanılması sağlanmalıdır.

Çıkarılabilir depolama ortamlarında kullanılan şifreleme algoritmaları dikkatlice seçilerek, endüstri standartlarına uygun güçlü şifreleme yöntemleri kullanılmalıdır. Bu, bilgilerin yetkisiz erişime karşı korunmasını sağlanmalıdır.

Firmamız, güvenlik politikaları çerçevesinde şifreleme anahtarlarının etkin bir şekilde yönetilmesini sağlamak üzere özel bir anahtar yönetimi politikası benimsemiştir.

Çıkarılabilir depolama cihazlarında bilgilerin şifrelenmemiş olarak depolanmasını önlemek amacıyla şifreleme zorunlu hale getirilmelidir. Bu uygulama, şifreleme olmayan cihazların kullanımını engelleyerek güvenlik standardını

yükseltmektedir. Dizüstü bilgisayarlar ve taşınabilir depolama cihazları için tam disk şifreleme çözümleri aktif olarak kullanılmalıdır. Bu sayede cihazlar kaybolduğunda veya çalındığında bile veriler güvence altına alınmaktadır.

Çalışanlara çıkarılabilir depolama cihazlarını güvenli bir şekilde kullanma konusunda düzenli eğitimler verilmelidir. Bu eğitimler, şifreleme anahtarlarının nasıl korunacağı ve cihazların güvenli bir şekilde kullanılması konularında farkındalık yaratmayı hedeflemektedir.

Şifrelenmiş depolama cihazlarından gelen olaylar, Bilgi İşlem ekibi tarafından düzenli olarak izlenerek incelenmelidir. Bu sayede olası güvenlik ihlalleri hızlı bir şekilde tespit edilerek önlemler alınmalıdır. Firmamız, bu uygulamaları titizlikle sürdürerek bilgilerin gizliliği ve bütünlüğünü en üst düzeyde koruma taahhüdünü sürdürmektedir.

Depolanan bilgiye hâlen ihtiyaç duyulurken depolama ortamının bozulma riskini azaltmak için bilgilerin okunamaz hale gelmeden önce yeni depolama ortamına aktarılması, önemli bir veri koruma ve iş sürekliliği stratejisidir. Hangi verilerin yedekleneceği, ne sıklıkla yedek alınacağı ve yedeklerin nasıl saklanacağı gibi konular doğrultusunda veri yedekleme çalışmaları gerçekleştirilmelidir.

Otomatik yedekleme sistemleri kullanılarak kritik verilerin belirlenen periyodlarla yedeklenmesini sağlanmalıdır. Bu sistemler, verilerin kaydedilmesi anında veya belirli zaman aralıklarında otomatik olarak yedek almaktadır.

Verilerin bozulması durumunda geri dönülebilecek stratejik noktalar belirlenerek veri yedeklemesi yapılmalıdır. Düzenli olarak veri yedekleme testleri gerçekleştirilmelidir. Bu testler, yedeklerin doğru bir şekilde alındığını ve kurtarma sürecinin işlevsel olduğunu doğrulamak için yapılır.

Yedekleme ortamları çoğaltılarak verilerin birden fazla depolama ortamında saklanmasını sağlanmalıdır. Bu sayede tek bir depolama ortamının bozulması durumunda diğer ortamlardan verilere erişim mümkün olmaktadır. Yedeklenen veriler şifrelenerek yetkisiz erişim durumunda bile verilerin okunması önlenmeli ve güvenliği sağlanmalıdır.

Veri yedekleme süreçleri düzenli olarak gözden geçirilerek iyileştirme fırsatları belirlenir. Teknolojik yenilikler ve güvenlik standartlarına uyum sağlamak için sürekli olarak güncelleme yapılmalıdır. Bu çalışmalar, firmamızın veri yedekleme ve depolama süreçlerini etkin bir şekilde yöneterek verilerin güvenliğini ve bütünlüğünü korumasına yardımcı olur.

Kritik verilerin güvenliği için birden fazla depolama ortamı kullanmalıdır. Bulut tabanlı depolama hizmetleri, harici sabit diskler ve ayrı sunucular gibi farklı ortamlar arasında veri dağılımı sağlanmalıdır. Kritik verilerin yedeklenmesi için çoğaltılmış yedekleme süreçleri kullanılmalıdır. Bu süreçler, farklı zamanlarda ve farklı depolama ortamlarına otomatik olarak yedekleme yaparak veri bütünlüğünü ve güvenliğini sağlamalıdır.

"Bilgi kaybı ihtimalini sınırlamak için çıkarılabilir depolama ortamının (kütüğe) kaydedilmesinin dikkate alınması", şirketin önemli bilgileri korumak için taşınabilir depolama cihazlarını kullanarak yedekleme yapılmaktadır. Bu kapsamda; uygun çıkarılabilir depolama ortamlarının belirlenmesi için bir standart oluşturulmuş ve kullanılacak medyanın dayanıklılığı, depolama kapasitesi, hızı ve güvenlik özellikleri gibi faktörler üzerinde detaylı değerlendirmeler yapılmalıdır. İlgili standartlar aşağıdaki gibidir.

USB Flash Sürücüler

- **Güvenilir Markalar:** Bilinen ve güvenilir markalardan seçilmiş USB flash sürücüler tercih edilmelidir. Örneğin, SanDisk, Kingston, Samsung gibi markalar güvenilir seçenekler arasındadır.
- **Dayanıklılık:** Metal kasa veya darbe emici özelliklere sahip modeller tercih edilmelidir.

- **Yüksek Kapasite:** İhtiyaçları karşılayacak yeterli depolama kapasitesine sahip olmalıdır. Örneğin, en az 64 GB veya daha fazla kapasiteye sahip modeller tercih edilebilir.

Harici Sabit Diskler

- **Güvenilir Markalar:** Bilinen ve güvenilir markalardan seçilmiş harici sabit diskler tercih edilmelidir. Örneğin, Seagate, Western Digital gibi markalar güvenilir seçenekler arasındadır.
- **Dayanıklılık:**. Özellikle darbe emici kasa veya kılıfı olan modeller seçilebilir.
- **Yüksek Kapasite:** İhtiyaçları karşılayacak yeterli depolama kapasitesine sahip olmalıdır. Örneğin, en az 1 TB veya daha fazla kapasiteye sahip modeller tercih edilebilir.

Optik Diskler (CD/DVD/Blu-ray)

- **Kaliteli Medya:** Veri depolamak için kaliteli CD, DVD veya Blu-ray diskler kullanılmalıdır. Düşük kaliteli veya uygun fiyatlı diskler veri kaybına neden olabilir.
- **Dayanıklılık:** Disklerin fiziksel olarak hasara karşı dayanıklı olması önemlidir. Özellikle çizilmelere karşı dayanıklı kaplamaya sahip diskler tercih edilmelidir.
- **Uygun Depolama Ortamı:** Optik diskler, toz, nem ve ısıdan korunacak uygun bir ortamda saklanmalıdır. Hijyenik bir ortam ve uygun depolama kutuları kullanılmalıdır.

Bu özellikler, çıkarılabilir depolama cihazlarının seçiminde dikkate alınması gereken temel noktalardır. Firmanın ihtiyaçları ve bütçesine uygun olan güvenilir, dayanıklı ve yüksek kapasiteli cihazlar tercih edilmelidir.

Bilgi güvenliğini sağlamak ve yetkisiz erişimi engellemek amacıyla çıkarılabilir depolama ortamı bağlantı noktalarının etkinleştirilmesi konusunda adımlar atılmalıdır. Bu adımlar, kurumsal güvenliği artırmak ve bilgi kaybı riskini azaltmak için yapılan stratejik bir çalışmadır. Bu kapsamda;

- **Çıkarılabilir Depolama Ortamı Bağlantı Noktalarının Kontrolü:** Şirket, bilgisayar ve diğer cihazlarda bulunan çıkarılabilir depolama ortamı bağlantı noktalarının (örneğin, USB ve SD kart yuvaları) kontrolünü sağlamak için yazılım tabanlı veya donanım tabanlı erişim kontrol mekanizmaları kullanmalıdır. Bu mekanizmalar, yetkisiz cihazların bağlanmasını engeller ve yalnızca yetkilendirilmiş cihazların kullanılmasına izin verir.
- **Güvenlik Yazılımları ve Donanımları:** Çıkarılabilir depolama ortamlarının güvenliğini artırmak için güvenlik yazılımları ve donanımları kullanılmalıdır. Bu yazılımlar ve donanımlar, cihazlara bağlanan çıkarılabilir depolama ortamlarını tarar, izler ve izinsiz erişim girişimlerini engeller.
- **Eğitim ve Farkındalık Programları:** Çalışanlara, çıkarılabilir depolama ortamlarının güvenli kullanımı konusunda düzenli eğitimler verilmelidir. Bu eğitimler, çalışanların bilinçlenmesini sağlayarak yanlışlıkla veya kasıtlı olarak güvenlik ihlallerini önlemeye yöneliktir.
- **İzleme ve Denetim:** Çıkarılabilir depolama ortamlarının bağlantı noktalarını izlenip ve denetlemelidir. Bu süreçler, olası güvenlik ihlallerini tespit etmek ve önlemek için düzenli olarak gerçekleştirilmelidir.

Çıkarılabilir depolama ortamının kullanılması durumunda bilgilerin aktarımını izleme stratejileri şu şekildedir;

- **İzleme Yazılımları ve Sistemlerin Kullanımı:** Bilgilerin çıkarılabilir depolama ortamına aktarımını izlemek için özel yazılımlar ve sistemler kullanılmalıdır. Bu yazılımlar, depolama cihazlarına veri aktarımını algılar ve kaydeder, böylece yetkisiz veri aktarımlarını tespit etmeye yardımcı olur.
- **Erişim Kontrol ve Yetkilendirme Politikaları:** Çıkarılabilir depolama ortamlarına erişim ve veri aktarımını sınırlamak için sıkı erişim kontrol ve yetkilendirme politikaları benimsenmelidir. Bu politikalar, sadece yetkilendirilmiş personelin bilgileri aktarmasına izin verir ve yetkisiz erişimi önler.
- **Otomatik Uyarı ve Alarm Sistemleri:** Çıkarılabilir depolama ortamlarına yapılan veri aktarımlarını izlemek ve anormal durumları tespit etmek için otomatik uyarı ve alarm sistemleri kullanılmalıdır. Bu sistemler, beklenmedik veya şüpheli veri aktarımlarını tespit ederek hızlı bir şekilde müdahale etmeyi sağlar.

BGYS POLİTİKASI

Bilgilerin fiziksel taşınması sırasında güvenliğini sağlamak amacıyla gerekli önlemleri alınmalıdır. Bilgilerin posta hizmeti veya kurye yoluyla depolama ortamını gönderilmesi durumunda yetkisiz erişime, kötüye kullanıma veya bozulmaya karşı savunmasız olmaması için gerçekleştirecek çalışmalar şunlardır;

- **Güvenli Ambalajlama ve Paketleme:** Bilgilerin taşınmasında fiziksel zarar görmesini önlemek için uygun ambalajlama ve paketleme yöntemleri kullanılmalıdır.
- **Güvenli Taşıma Şirketleri ile İşbirliği:** Şirket, bilgilerin taşınması için güvenilir ve güvenli taşıma şirketleriyle işbirliği yapılmalıdır. Bu şirketlerin güvenlik standartlarına uygun olduğu doğrulanmalı ve bilgilerin güvenli bir şekilde taşınması sağlanmalıdır.
- **Teslimat Onayı ve Alıcının Kimliğinin Doğrulanması**: Bilgilerin teslimatı sırasında alıcının kimliği doğrulanmalı ve teslimatın alındığına dair resmi bir onay alınmalıdır.