BATISÖKE BİLGİ GÜVENLİĞİ POLİTİKASI

1. Giriş: Politikanın Amacı, Kapsamı ve Dayanağı

Stratejik Bağlam

Bu politika, Batı Anadolu Şirketler Topluluğu bünyesinde yer alan halka açık şirketi olan Batısöke Söke Çimento Sanayii T.A.Ş.'nin ("Şirket") bilgi varlıklarını koruma taahhüdünü ve bu konudaki kurumsal yönetim yaklaşımını ortaya koymaktadır.

Bilgi sistemlerinin güvenli, kesintisiz ve mevzuata uygun şekilde yönetilmesi, sermaye piyasası düzenlemeleri çerçevesinde paydaşlarımıza karşı sorumluluğumuzun temel bir parçasıdır. Bu politika, Şirket'in maruz kalabileceği operasyonel, finansal ve itibar risklerini en aza indirerek sürdürülebilir başarıyı destekleyen stratejik bir çerçeve sunar.

Politikanın Amacı

Bu politikanın temel amacı, Şirket'in bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini en üst düzeyde korumaktır. Bu doğrultuda, bilgi sistemlerine ilişkin yönetişim yapısı ve sorumluluklar tanımlanmakta, bilgi güvenliği risklerinin yönetilmesine yönelik esaslar belirlenmektedir.

Politika, bilgi sistemleri kontrollerinin tesis edilmesini ve bu kontrollerin sürekliliğinin sağlanmasını hedefleyerek, Şirket'in yasal uyumluluğunu güvence altına almayı ve risklerini asgari seviyeye indirmeyi amaçlar.

Kapsam

Politika; Şirket'in sahip olduğu, kullandığı veya üçüncü taraflar aracılığıyla hizmet aldığı tüm bilgi sistemlerini, bilgi teknolojileri altyapılarını, uygulamaları, veri tabanlarını, elektronik ortamda tutulan bilgileri ve bu sistemleri kullanan çalışanları kapsar. Şirket adına bilgi işleyen dış hizmet sağlayıcılar ve üçüncü taraflar da sözleşmeler çerçevesinde bu politika hükümlerine tabidir.

Yasal Dayanak

Bu politika; SPK'nın VII-128.10 sayılı Tebliği, 6698 sayılı KVKK, Türk Ticaret Kanunu ve ilgili diğer mevzuat esas alınarak hazırlanmıştır. Politika hükümleri, Tebliğ'de yer alan risk esaslı ve orantılılık ilkesi çerçevesinde uygulanır.

2. Yönetişim Yapısı ve Sorumluluklar

Yönetim Kurulu

- Bilgi Güvenliği Politikası'nı onaylar ve uygulanmasını gözetir.
- Bilgi sistemleri kontrollerinin yeterliliğini değerlendirir.
- Bilgi sistemlerinden kaynaklanan riskleri dikkate alarak stratejik kararlar alır.

Üst Yönetim

- Politikanın Şirket genelinde uygulanmasını sağlar ve gerekli kaynakları tahsis eder.
- Bilgi sistemleri risklerinin yönetimini, ihlallerin takibini ve personele yıllık eğitim verilmesini gözetir.
- Yeni bilgi sistemleri ve kritik projeleri riskler çerçevesinde değerlendirerek onaylar.
- En az 5 yıl tecrübeli bir Bilgi Güvenliği Sorumlusu atar.

Bilgi Güvenliği Sorumlusu

- Bilgi güvenliği yönetim sisteminin kurulmasından, uygulanmasından ve sürekliliğinden sorumludur.
- Güvenlik açıkları, yamalar ve olay yönetimi süreçlerini izler.
- Uzaktan erişim, ayrıcalıklı yetkiler ve benzeri kritik konularda onay ve gözetim rolü üstlenir.
- Görevini üst yönetime bağlı ve bağımsız şekilde yürütür.

Birim Yöneticileri ve Çalışanlar

- Birim yöneticileri, kendi alanlarındaki bilgi varlıklarının korunmasını sağlar.
- Çalışanlar, sistemleri yalnızca yetkileri kapsamında kullanır ve ihlalleri derhal bildirir.

3. Bilgi Güvenliği Temel İlkeleri

Risk Yönetimi

Bilgi sistemlerine ilişkin riskler yılda en az bir kez ve önemli değişiklikler sonrasında analiz edilir; sonuçlar Üst Yönetim tarafından değerlendirilir.

Bilgi Varlıkları ve Erişim Yönetimi

Bilgi varlıkları için envanter oluşturulur ve sınıflandırılır. Erişim yetkileri en az yetki ilkesine göre verilir ve düzenli gözden geçirilir. Kimlik doğrulama mekanizmaları risk seviyesine uygun şekilde yapılandırılır ve kritik sistemler için çok faktörlü kimlik doğrulama uygulanır.

Kimlik Doğrulama ve Yetkilendirme

Kimlik doğrulama mekanizmaları risk seviyesine uygun şekilde yapılandırılır; kritik sistemler ve ayrıcalıklı hesaplar için çok faktörlü kimlik doğrulama uygulanır.

Kayıt ve İzleme

Bilgi sistemleri üzerinde gerçekleştirilen kritik işlemler, erişimler ve değişiklikler kayıt altına alınır; bu kayıtlar yetkisiz erişime karşı korunur ve gerektiğinde denetim ve inceleme amacıyla kullanılır.

Fiziksel ve Çevresel Güvenlik

Kritik bilgi teknolojisi varlıkları güvenli alanlarda bulundurulur ve bu alanlara erişimler kontrol altında tutulur.

İş Sürekliliği ve Olay Yönetimi

Bilgi sistemleri süreklilik planları hazırlanır ve düzenli olarak test edilir. Bilgi güvenliği ihlallerine yönelik Olay Müdahale Planı uygulanır.

Dış Kaynak ve Üçüncü Taraf Yönetimi

Hizmet sağlayıcılarla yapılan sözleşmelerde bilgi güvenliği ve gizlilik yükümlülükleri tanımlanır.

Yasal Uyum

Politika ve uygulamalar yürürlükteki mevzuata uygun yürütülür. Saklama süresi sona eren veriler, ilgili mevzuata uygun şekilde güvenli ve geri döndürülemez biçimde silinir veya imha edilir.

4. Politika Uygulama ve Yürürlük

Kullanıcı Farkındalığı ve Eğitimi

Şirket personeline, bilgi güvenliği politikası, uymaları gereken kurallar ve bilgi güvenliği ihlali durumlarında izlenecek süreçler hakkında yılda en az bir kez farkındalık ve bilgilendirme eğitimi verilir. Eğitimler, personelin görev ve sorumlulukları dikkate alınarak planlanır ve bilgi güvenliği kültürünün kurum genelinde yerleşmesi hedeflenir.

Olağandışı Durumlarda Harcamalar ve Onay

Bilgi güvenliği kapsamında olağandışı durumlarda yapılacak harcamalar için genel bütçe çerçevesi oluşturulur. Şirket içi yetki ve imza esasları çerçevesinde gerekli hallerde Yönetim Kurulu onayı alınır.

Politikanın Gözden Geçirilmesi

Bilgi Güvenliği Politikası, değişen iş ihtiyaçları, teknolojik gelişmeler, ortaya çıkan yeni tehditler ve mevzuat değişiklikleri dikkate alınarak yılda en az bir kez gözden geçirilir. Gerekli görülen hallerde politika güncellenir ve onay süreçlerine sunulur.

Onay ve Yürürlük

Bu Politika, Yönetim Kurulu onayıyla yürürlüğe girer. Politikada yapılacak değişiklikler de Yönetim Kurulu onayına tabidir. Güncel politika metni çalışanlara ve ilgili paydaşlara duyurulur.