P-5.1 KAPSAM VE BİLGİ GÜVENLİĞİ POLİTİKASI

1. KAPSAM

1.1. BGYS' nin Kapsamı

BGYS'nin kapsamı Unimar'daki tüm bilgi işlem ve endüstriyel bilgi işlem hizmetleridir. BGYS Unimar' de Veri Merkezinde ve erişim noktalarındaki donanım ve yazılımlardan oluşan kritik bilgi varlıklarının güvenliğini sağlamak üzere oluşturulmuştur. İşin karakteristik özelliği iletişim ve data hatlarının hizmet bakımından sürekliliğinin sağlanması olduğu için buna ait organizasyon, yer, varlıklar ve teknoloji sistem içine dahil edilmiştir. Unimar Bilgi Güvenliği Politikası, "Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması" yönetmeliği ile uyumludur.

1.2. Tanımlar

ISO27001:2013'te kullanılan terimler burada kullanıldığında, o standardın 3. maddesinde sağlanan tanımlar geçerlidir. Terimler ISO27002:2013'te tanımlı olup ISO27001:2013'te tanımlı olmadığında, burada ISO27002:2013 tanımları geçerlidir.

1.3. Bilgi Güvenliği Yönetim Sistemi ("BGYS"), bir iş riski yaklaşımına dayanan, Unimar içinde yönetimin bilgi güvenliğini kurmasına, uygulamasına, işletmesine, izlemesine, değerlendirmesine, idame ettirmesine ve geliştirmesine olanak veren, (kurumsal yapıyı, politikaları, planlama aktivitelerini, planları, sorumlulukları, çalışma uygulamalarını, prosedürleri, süreçleri ve kaynakları içermek suretiyle) Unimar' de genel yönetim sisteminin bir parçası olarak tanımlanır.

1.4. Güvenlik İhlali Kurumun fiziksel veya elektronik bilgi varlıklarının kullanılabilirliği, gizliliği veya bütünlüğünde bir bozulmaya neden olan veya olabilecek olay veya etkinliklerdir.

2. BİLGİ GÜVENLİĞİ POLİTİKASI

Kontrol hedefi: Unimar, iş gereksinimleri ile ilgili kanun ve düzenlemelere uygun olarak bilgi güvenliği için yönetim yönlendirmesi ve destek sağlar.

2.1. Bilgi güvenliği politikası dokümanı

Yönetim ekibi, Unimar için bir bilgi güvenliği politikası onaylamıştır. Bu politika aşağıda düzenlenmiş ve Genel Müdür'ün imzası altında, dağıtılmak üzere onaylanmıştır. Bu dokümanın güncel versiyonu tüm personel, yükleniciler ve şirket dışı taraflar için kullanılabilir durumdadır.

Bilgi güvenliği politikası

Sultanköy Mevkii, Marmara Ereğlisi, Tekirdağ adresinde bulunan UNIMAR A.Ş, Enerji sektöründe faaliyet göstermektedir.

Unimar' de BGYS kurulması aracılığı ile kurum için riskleri tanımlamak, belirlemek, değerlendirmek ve kontrol etmek olanaklı olmaktadır. Mevcut risk yönetimi çerçevesi ile risk değerlendirme ve risk müdahale planı bilgi ile ilgili risklerin nasıl kontrol edildiğini açıklamaktadır. Bilgi Güvenliği Yöneticisi risk müdahale planının yönetiminden sorumludur. BGYS ile gerekli olduğunda belirli riskler için ek risk değerlendirmeleri, yürütülebilir ve ilave uygun kontroller oluşturulabilir.

Unimar' de bilgi güvenliği gereksinimleri kurumsal hedefler ile aynı doğrultuda olacaktır ve BGYS' nin, bilgi ile ilgili riskleri kabul edilebilir düzeylere indirmek için, bilgi paylaşımı olanağı veren bir mekanizma olması hedeflenmiştir.

Unimar' de iş sürekliliği planı, veri yedekleme prosedürleri, virüslerden ve bilgisayar korsanlarından sakınma, erişim kontrolü ve bilgi güvenliği ihlal bildirimi, bu politika için esastır. Bu alanların her biri için kontrol hedefleri yazılı politikalar ve prosedürler ile desteklenir.

Unimar, Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunmasını taahhüt eder.

Unimar yönetimi, kurumun yasal, düzenleyici uygunluğunu korumak amacıyla, kurum çapında gizliliği, bütünlüğü ve tüm fiziksel ve sanal bilgi varlıklarını koruma taahhüdünde bulunmuştur.

Tüm Unimar çalışanlarının ve BGYS'nde tanımlanan belirli kurum dışı tarafların bu politikaya ve bu politikayı uygulayan BGYS'ne uymaları beklenmektedir. Tüm personel ve belirli şirket dışı taraflar, uygun eğitimi alacaklardır.

BGYS, sürekli ve sistematik değerlendirme ve geliştirmeye tabidir.

Unimar, BGYS çerçevesini desteklemek ve güvenlik politikasını periyodik olarak gözden geçirmek amacıyla, üst yönetim tarafından yönetilen ve Bilgi Güvenliği Yöneticisi ile diğer yöneticilerin dahil olduğu bir bilgi güvenlik komitesi oluşturmuştur.

Unimar kendi BGYS'nin, ISO27001:2013 onay belgesini elde etmeyi taahhüt etmiştir.

Bu politika, risk değerlendirmede veya risk müdahale planındaki değişikliklere yanıt vermek amacıyla yılda en az bir kez gözden geçirilecektir.

2.2. Bilgi güvenliği politikasının değerlendirilmesi

Unimar' de bilgi güvenliği politikası, uygunluğunun, yeterliliğinin ve etkinliğinin sürekli olarak sağlanması için düzenli aralıklarla veya büyük değişiklikler meydana geldiğinde gözden geçirilir

2.3. Bilgi Güvenliği Yöneticisi, bilgi güvenliği politikasının yöneticisidir ve politikanın geliştirilmesi, gözden geçirilmesi ve değerlendirilmesi için yönetim sorumluluğunu onaylamıştır.

2.4. Unimar, bilgi güvenliği politikasının yönetim değerlendirmesi için bir prosedür (MAR STN LMS REV 4) tanımlamıştır ve buna sürekli geliştirme ve kurumsal ortamda, iş çevrelerinde, yasal koşullarda veya teknik ortamda meydana gelebilecek önemli değişikliklere yanıt vermek için gerekli olabilecek politika değişikliklerini değerlendirmek dahildir.

2.5. Bilgi güvenliği politikasında yapılacak tüm değişiklikler Unimar' de İcra Komitesi'nin onayına tabidir.

BGYS Bilgi Güvenliği Yönetim Sistemidir ve bu politika, ve diğer destekleyici ve ilgili belgeler bu sistemin birer parçasıdır ve sistem ISO27001:2013'te belirtilen teknik özellikler ile uyumlu olarak tasarlanmıştır.

Bu doküman Bilgi Güvenliği Yöneticisi' nin sorumluğu altındadır ve BGYS' nin tüm gereklerini karşılamak üzere hazırlanmıştır

Dokümanın güncel sürümü üst yönetimce belirlenmiş tüm personelin kullanımına ve gözden geçirmesine açıktır. Gizli bilgi içermemektedir ve ilgili üçüncü şahıslarla paylaşılabilinir.