YYS CERTIFICATION		**Belgelendirme Danışmanlık** *Certification Consultancy*	
ISO 27001	**TÜRKAK**	**Tarih**/ *Date*	21.03.2017
Kuruluş / *Organization*	*YYS DANIŞMANLIK*		
Adres / *Adress*	*Yenibosna Merkez Mah. 29.Ekim Cad. No:35 Bahçelievler/İSTANBUL*		
Telefon / *Phone*	*+90 212 541 25 53*	***Cep*** *+90 533 814 39 61*	

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi

Bilgi Güvenliği konusunda, hangi bilgi varlıklarımızın olduğunu, bu varlıkların değerinin farkına vararak onları bir sistem sayesinde koruyabilme ve kuracağımız kontroller ile koruma metotlarını belirlenmesine yardımcı olur. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Bilgi, kuruluşunuzun faaliyetleri ve belki devamı için büyük bir önem taşır. ISO/IEC 27001 Belgesi değerli bilgi varlıklarınızı yönetmenize ve korumanıza yardımcı olur. ISO/IEC 27001, Bilgi Güvenliği Yönetimi Sistemi (ISMS) gereksinimlerini tanımlayan tek uluslararası denetlenebilir standarttır. Yeterli ve orantılı güvenlik denetimleri seçilmesini sağlamak için tasarlanmıştır.

Bu standard, bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) (Information Security Management System -ISMS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. Bir kuruluş için BGYS'nin benimsenmesi stratejik bir karar olmalıdır.

Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler ve kuruluşun büyüklüğü ve yapısından etkilenir.

Bilgi, organizasyonlara değer katan ve bu nedenle uygun şekilde korunması gereken kaynaklar olarak tanımlanabilir. Günümüzde bilgi başta basılı, sözlü, elektronik ortamlar olmak üzere birçok yerde bulunmakta, saklanmakta, posta ve e-mail gibi birçok yolla transfer edilebilmektedir.

Bilgi güvenliği, iş devamlılığını sağlamak, meydana gelebilecek zararı en aza indirebilmek, kazancın ve iş fırsatlarının artırılması amacıyla bilgiyi birçok tehlikeye karşı korumayı hedefler.

ISO/IEC 27001, Bilgi Güvenliği Yönetimi Sistemi (ISMS) gereksinimlerini tanımlayan tek uluslararası denetlenebilir standarttır. Yeterli ve orantılı güvenlik denetimleri seçilmesini sağlamak için tasarlanmıştır.

Bu, bilgi varlıklarınızı korumanıza ve ilgili taraflara, özellikle de müşterilerinize güven vermenize yardımcı olur. Bu standart, Bilgi Güvenliği Yönetimi Sisteminizi oluşturmak, uygulamak, işletmek, izlemek, incelemek, sürdürmek ve geliştirmek için süreç yaklaşımını benimser.

Standarta göre her türlü formda bilginin korunması ve saklanması esastır, özellikle de müşterinize ait bilgileri gizlemekten sorumluysanız. Bunun gerçekleştirilmemesi, ticari kayıp ve itibar kaybı anlamına gelir bu da pahalı bir hukuk davasıyla sonuçlanabilir.

ISO 27001:2005, muhafaza edilen bilginin güvenilirliğini, gizliliğini ve geçerliliğini garantilemede koruma ve kontrol sağlar.

ISO 27001:2005, Bilgi Güvenliği Yönetim Sistemi (BGYS) için esas oluşturur ve tüm sektörlerdeki her ölçekte kuruluşa uygulanır. BGYS Sertifikası sizin müşterilerinize, tedarikçilerinize ve devlet kurumlarına karşı sizin Bilgi Güvenliği için sağladığınızı gösterir.

Bu nedenle bilgi güvenliği, kuruluşunuzun faaliyetleri, hatta belki devamı için büyük önem taşır. ISO/IEC 27001 sertifikasyon (belgelendirme)u, değerli bilgi varlıklarınızı yönetmenize ve korumanıza yardımcı olur.

Bilgi Güvenliği Nedir

Günümüzde ticari şirketler ve devlet kurumları işlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin önemi artmış, sadece güvenli bir şekilde saklanması ve depolanması gelişen ihtiyaçlara cevap verememiş aynı zamanda bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline gelmiştir. Bilgiye olan bu bağımlılık bilginin korunması ihtiyacını gündeme getirmiştir. Bu anlamda bilgi, kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahiptir. Bilgiye yönelik olası saldırılar, tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, bilgi altyapısının bozulmasına ve bu da beraberinde işlerin aksamasına neden olmaktadır. Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar.

Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür.

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

1. *Gizlilik (Confidentiality)*
2. *Bütünlük (Integrity)*
3. *Kullanılabilirlik (Availability)*

Bu kavramları biraz daha açacak olursak gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir. Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz. Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır.

Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Nedir

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), bilgi güvenliğini yönetim sistemi olarak tanımlayan uluslararası denetlenebilir bir standarttır. Bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanmıştır.

Bu Yönetim Sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi, her sektör ve büyüklükteki kuruluşa uygulanabilen bir standarttır. Bu standart, dokümante edilmiş bir BGYS' yi, kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek gereksinimlerini kapsar. Günümüzde kuruluşlar için değerli olan bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından korunması, süreklilik ve sistematikliği gerekmektedir.

Koruma, bir takım fiziksel ve sistemsel önlemlerin yanında bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika ya da kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası riskleri mümkün olabilecek en düşük risk düzeyinde nasıl tutabileceği konusunda bilgilendirilmesiyle mümkün olmaktadır. Bir kuruluş için Bilgi Güvenliği Yönetim Sistemi'nin benimsenmesi stratejik bir karar olmalıdır. Kuruluş, yönetim sisteminin tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler, kuruluşun büyüklüğü ve yapısından etkilenir. ISO 27001 ile kuruluşlar uygulayacağı güvenlik kontrollerini belirler.

FAYDALARI

1. *Bilgi varlıklarının farkına varma: Kuruluş hangi bilgi varlıklarının olduğunu, değerinin farkına varır.*
2. *Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile koruma metotlarını belirler ve uygulayarak korur.*
3. *İş sürekliliği: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.*
4. *İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgilen korunacağından ilgili tarafların güvenini kazanır.*
5. *Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.*
6. *Müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.*
7. *Çalışanların motivasyonunu arttırır.*
8. *Yasal takipleri önler.*
9. *Yüksek prestij sağlar.*

ISO/IEC 27001 İle ilgili Terim ve Kavramlar

- *Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.*
- *Risk analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı.*
- *Risk değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses.*
- *Risk derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi.*
- *Risk yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler.*
- *Risk işleme: Riski değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanması prosesi.*
- *Uygulanabilirlik bildirgesi: Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildir.*

ISO 27001 nedir?

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), bilgi güvenliğini yönetim sistemi olarak tanımlayan uluslararası denetlenebilir bir standarttır. Bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanmıştır.

Bu Yönetim Sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi, her sektör ve büyüklükteki kuruluşa uygulanabilen bir standarttır.

Bu standart, dokümante edilmiş bir BGYS' yi, kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek gereksinimlerini kapsar.

Günümüzde kuruluşlar için değerli olan bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından korunması, süreklilik ve sistematikliği gerekmektedir.

Koruma, bir takım fiziksel ve sistemsel önlemlerin yanında bireylerin bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika ya da kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası riskleri mümkün olabilecek en düşük risk düzeyinde nasıl tutabileceği konusunda bilgilendirilmesiyle mümkün olmaktadır.

Bir kuruluş için Bilgi Güvenliği Yönetim Sistemi'nin benimsenmesi stratejik bir karar olmalıdır. Kuruluş, yönetim sisteminin tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler, kuruluşun büyüklüğü ve yapısından etkilenir.

ISO 27001 ile kuruluşlar uygulayacağı güvenlik kontrollerini belirler.

Bilgi Güvenliği Nedir

Bilginin gizliliği, bütünlüğü¨ ve kullanılabilirliğinin korunmasıdır. Geniş kapsamda; doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsamaktadır.

Bilgi güvenliği, kurumdaki işlerin sürekliliğinin sağlanması, meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin çok yönlü tehditlerden korunmasını sağlar. Kuruluşlarda bilgi birçok biçimde bulunmaktadır. Kağıt üzerinde, elektronik ortamda, posta yada elektronik posta yolu ile bir yerden bir yere iletilebilir ya da kişiler arası sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun bir şekilde korunmalıdır.

ISO 27001 Neden Gereklidir?

Bilgi Güvenliği Yönetim Sistemi Faydaları Nelerdir

İç denetimlerinizin bağımsız bir şekilde sağlandığını gösterir ve kurumsal yönetişim ve iş devamlılığı gereksinimlerini karşılar. Kuruluşa yönelik faydaları;

- *Bilgi varlıklarının gizliliğinin korunması,*
- *Tehdit ve riskleri belirlenerek etkin bir risk yönetiminin sağlanması,*
- *Kurumsal prestijin korunması,*
- *İş sürekliliğinin sağlanması,*
- *Bilgi kaynaklarına erişimin denetlenmesi,*
- *Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda farkındalık düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi,*
- *Otomatik ve elle yönetilen sistemlerde, duyarlı bilgilerin uygun bir şekilde kullanıldığının garanti altına alınması amacıyla gerçekçi bir kontrol sistemi kurulması,*
- *Bilgi varlıklarının bütünlüğünün ve doğruluğunun sağlanması,*
- *Personelin, başkaları tarafından yapılabilecek olan suiistimal ve tacizlere karşı zan altında kalmasının engellenmesi,*
- *Duyarlı bilgilerin uygun bir şekilde üçüncü taraflara ve denetçilere açık olmasının sağlanmasıdır.*
- *Geçerli yasa ve düzenlemelere uygun davranıldığını bağımsız bir şekilde gösterir.*
- *Sözleşmeden doğan gereklilikleri karşılayarak ve müşterilerinize bilgilerinin güvenliğine gösterdiğiniz özeni göstererek bir rekabet avantajı sağlar.*
- *Bilgi güvenliği işlemleriniz, prosedürleriniz ve belgeleriniz biçimlendirilirken kurumsal risklerinizin gerektiği gibi tanımlandığını, değerlendirildiğini ve yönetildiğini bağımsız bir şekilde doğrular.*
- *Düzenli değerlendirme işlemi performansınızı sürekli izlemenize ve geliştirmenize yardımcı olur. Üst yönetiminizin bilgilerinin güvenliğine olan taahhüdünü kanıtlar.*

- *Kurum ve kurum çalışanları bilgi güvenliği sistemi ile;*
- *Bilgi varlıklarının farkındalılığı ve motivasyonu artar,*
- *Sahip olduğu bilgi varlıkları korunabilir*
- *İş sürekliliği sağlanır,*
- *Müşteri ve tedarikçilerle sağlıklı bir yapı kurulur,*
- *Rekabette avantaj sağlanır,*
- *Yasal uyumluluk sağlanır.*

Bilgi Güvenliği Yönetim Sistemi Prosesleri Nelerdir

ISO 27001 kuruluşun BGYS'sini kurmak, gerçekleştirmek, işletmek, izlemek, sürdürmek ve iyileştirmek için bir proses yaklaşımını benimser.

ISO 27001 Nasıl Alınır?

ISO 27001 Bilgi Güvenliği Yönetim Sistemleri belgelendirilmesi, kuruluşun kurmuş olduğu Bilgi güvenliği yönetim sistemlerinin bağımsız ve akredite bir sertifikasyon (belgelendirme) kuruluşunun denetiminden başarıyla geçmesi ve bunun devamlılığını sağlaması ile mümkündür. Kuruluş, Bilgi Güvenliği Yönetim Sistemi standardın gereksinimlerini karşılayacak şekilde kurduktan sonra, bu sistemin belgelendirilmesi için bir sertifikasyon (belgelendirme) kuruluşu ile anlaşır. Sertifikasyon (belgelendirme) kuruluşu, kuruluşun bilgi güvenliği sisteminin standardın gereksinimlerini karşılayıp karşılamadığını tespit etmek üzere bir sertifikasyon (belgelendirme) denetimi yapar. Bu denetim sonucunda sertifikasyon (belgelendirme) kuruluşu, kurulmuş olan bilgi güvenliği sisteminin ilgili standardın gereksinimlerinin yeterince karşılandığına karar verirse, kuruluşun bilgi güvenliği sistemini belgelendirir.

Böylece kuruluş iso belgesi nin kullanım haklarına sahip olur .Kuruluşun bilgi güvenliği sistemini belgelendirilmesinin ardından Sertifikasyon (belgelendirme) Kuruluşu, kuruluşun standardın gereklerini yerine getirmeye devam edip etmediğini tespit etmek üzere belirlenmiş aralıklarla takip denetimleri yapar. Kuruluşun Bilgi güvenliği yönetim sistemlerine verilmiş olan bu belge, aslında tamamen sertifikasyon kuruluşunun malı olup belirli bir süre için kuruluşa ödünç verilmiştir. Yapılan bu takip denetimleri sonucunda Sertifikasyon (belgelendirme) Kuruluşu, kuruluşun bilgi güvenliği sisteminin standardın gereklerini yeterince sağlamadığı kararına varırsa, kuruluşa ödünç vermiş olduğu iso 27001 belgesi ni geri alabilir.

ISO 27001 Belgesi Neden Alınır

- *Bilgi varlıklarının farkına varma: Kuruluş ISO 27001 Bilgi Güvenliği Yönetim Sistemi sayesinde hangi bilgi varlıklarının olduğunun ve bunların değerinin farkına varır.*
- *Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile ISO 27001 Bilgi Güvenliği Yönetim Sistemi sayesinde koruma metotlarını belirler ve uygulayarak korur.*
- *İş sürekliliği: ISO 27001 Bilgi Güvenliği Yönetim Sistemi firmanın uzun yıllar boyunca işini garanti eder. Ayrıca ISO 27001 Bilgi Güvenliği Yönetim Sistemi bir felaket halinde, işe devam etme yeterliliğine sahip olur.*
- *İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, ISO 27001 Bilgi Güvenliği Yönetim Sistemi sayesinde bilgileri korunacağından ilgili tarafların güvenini kazanır.*
- *ISO 27001 Bilgi Güvenliği Yönetim Sistemi bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.*
- *ISO 27001 belgesi ile Bilgi Güvenliği Yönetim Sistemi kuran firmaları müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.*
- *ISO 27001 Bilgi Güvenliği Yönetim Sistemi çalışanların motivasyonunu arttırır.*
- *ISO 27001 Bilgi Güvenliği Yönetim Sistemi yasal takipleri önler.*
- *ISO 27001 belgesi Bilgi Güvenliği Yönetim Sistemi yüksek prestij sağlar.*

ISO 27001 Belgesi Ne Kadar Sürede Alınır

Standart, sistemin kurulması ve dokümante edilmesi için gerekli genel kuralları tanımlar. Bir ürüne ait değildir. Bu nedenle firma veya kurum , kendi sektörüne göre standardı uygulamak zorundadır. ISO 27001 Standardının firma veya kuruma adapte edilmesi; yapısına, personel sayısına, fonksiyonel durumuna ve yönetiminin inanmasına bağlı

olarak uzun veya kısa zaman alabilir. Ayrıca sistem kurucunun (firma veya kurum içinden bir personel veya personel grubu ya da danışman kuruluş olabilir) konuya vakıf ve disiplini de süreyi etkiler.

ISO 27001 Faydaları Nelerdir?

İç denetimlerinizin bağımsız bir şekilde sağlandığını gösterir ve kurumsal yönetişim ve iş devamlılığı gereksinimlerini karşılar.

Kuruluşa yönelik faydaları;

- *Bilgi varlıklarının gizliliğinin korunması,*
- *Tehdit ve riskleri belirlenerek etkin bir risk yönetiminin sağlanması,*
- *Kurumsal prestijin korunması,*
- *İş sürekliliğinin sağlanması,*
- *Bilgi kaynaklarına erişimin denetlenmesi,*
- *Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda farkındalık düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi,*
- *Otomatik ve elle yönetilen sistemlerde, duyarlı bilgilerin uygun bir şekilde kullanıldığının garanti altına alınması amacıyla gerçekçi bir kontrol sistemi kurulması,*
- *Bilgi varlıklarının bütünlüğünün ve doğruluğunun sağlanması,*
- *Personelin, başkaları tarafından yapılabilecek olan suiistimal ve tacizlere karşı zan altında kalmasının engellenmesi,*
- *Duyarlı bilgilerin uygun bir şekilde üçüncü taraflara ve denetçilere açık olmasının sağlanmasıdır.*
- *Geçerli yasa ve düzenlemelere uygun davranıldığını bağımsız bir şekilde gösterir.*
- *Sözleşmeden doğan gereklilikleri karşılayarak ve müşterilerinize bilgilerinin güvenliğine gösterdiğiniz özeni göstererek bir rekabet avantajı sağlar.*
- *Bilgi güvenliği işlemleriniz, prosedürleriniz ve belgeleriniz biçimlendirilirken kurumsal risklerinizin gerektiği gibi tanımlandığını, değerlendirildiğini ve yönetildiğini bağımsız bir şekilde doğrular.*
- *Düzenli değerlendirme işlemi performansınızı sürekli izlemenize ve geliştirmenize yardımcı olur. Üst yönetiminizin bilgilerinin güvenliğine olan taahhüdünü kanıtlar.*

Kurum ve kurum çalışanları bilgi güvenliği sistemi ile;

- *Bilgi varlıklarının farkındalılığı ve motivasyonu artar,*
- *Sahip olduğu bilgi varlıkları korunabilir*
- *İş sürekliliği sağlanır,*
- *Müşteri ve tedarikçilerle sağlıklı bir yapı kurulur,*
- *Rekabette avantaj sağlanır,*
- *Yasal uyumluluk sağlanır.*

Bilgi Güvenliği Yönetim Sistemi Prosesleri Nelerdir

ISO 27001 kuruluşun BGYS'sini kurmak, gerçekleştirmek, işletmek, izlemek, sürdürmek ve iyileştirmek için bir proses yaklaşımını benimser.

ISO 27001in Yararları Nelerdir

ISO 27001'in Yararları

Bilgi varlıklarının farkına varma: Kuruluş hangi bilgi varlıklarının olduğunu, değerinin farkına varır. Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile koruma metotlarını belirler ve uygulayarak korur. İş sürekliliği: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur. İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.

Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz. Müşterileri değerlendirirse, rakiplerine göre daha iyi

değerlendirilir. Çalışanların motivasyonunu arttırır. Yasal takipleri önler Yüksek prestij sağlar.

ISO 27001 Belgelendirme Prosedürü

BELGELENDİRME PROSEDÜRÜ AŞAĞIDAKİLERİ İÇERİR

- *Bilgi formunun doldurulması*
- *Teklif verilmesi*
- *Sertifika için başvurulması*
- *Dökümanların gözden geçirilmesi*
- *Ön denetim (opsiyonel)*
- *Şirket denetimi*
- *Belgelendirme Komitesinin onayı*
- *Belgenin verilmesi*
- *Periyodik takip denetimleri*
- *Belge Yenileme*

ISO 27001 Bilgi Güvenliği Belgelendirme Süreci

Döküman İnceleme: Belgelendirme talebiniz alındıktan sonra müracaat için gerekli ek evraklar ve ilgili yönetim sistemine ait dokümanların firmamıza iletilmesi sağlanmalıdır.

Kuruluşunuza ait dokümanlar

ISO 27001 standardına uygunluk açısından incelenecek ve düzeltilmesi gereken bir durum olması halinde, bir rapor ile tarafınıza bildirilecektir.

Belgelendirme firmasına tarafından incelenmesi sonrasında, dokümanlarda söz konusu olabilecek değişiklikler, belgelendirme denetimi öncesinde tamamlanmalı ve Belgelendirme firmasına ulaştırılmalıdır.

Belgelendirme Denetimi: Belgelendirme denetimi, ISO 27001:2005 Belgelendirme denetiminin sonucunda sisteminizin standarda uygunluğunun tespit edilmesi durumunda kuruluşunuz ISO 27001:2005 belgesini almaya hak kazanacaktır. Kuruluş belgelendirme denetimini başarıyla tamamlanmasını takiben, denetim ekibimiz tarafından, belge verilmesi için önerilecektir. Bu aşamadan sonra, en kısa süre içinde belgeniz düzenlenerek tarafınıza sunulacaktır.

ISO 27001:2005 standardı ve sistem dokümanlarını uygunluğu tespit etmek amacı ile firmamızın denetim ekibi tarafından gerçekleştirilecektir. Belgelendirme denetiminin süresi firmanızın faaliyet kapsamı ve çalışan sayısı göz önünde bulundurularak uluslararası akreditasyon kurallarına göre belirlenecek ve denetim öncesinde bir program halinde bildirilecektir.

Takip Denetimi: Belgelendirme veya gözetim denetimlerinde sistemin genel işleyişini etkileyecek derecede, uygunsuzluk (lar) tespit edilmesi durumunda gerçekleştirilecek denetimlerdir. Takip denetimleri, belgelendirme ve ya gözetim denetimini gerçekleştiren denetim ekibi tarafından gerçekleştirilecektir.

Gözetim Denetimleri: Gözetim denetimleri kuruluşunuzun ISO 27001:2005 standardına uygunluğunun devamını kontrolü amacı ile en az yılda 1 olmak üzere gerçekleştirilecektir.

Belgelendirme Geçerlilik Süresi: ISO 27001:2005 standardına göre yapılan belgelendirme için belge geçerlilik süresi 3 (üç) yıldır.