1. AMAÇ

İşbu Kişisel Verilerin Korunması Uyum Süreci Politikası ("Politika"), Gaziantep Sanayi Odası ("GSO") nezdinde gerçekleştirilen veri işleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("Kanun") ilgili hükümleri uyarınca hukuka uygun şekilde yerine getirilmesi ve Kanun'un 12 inci maddesi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla hazırlanmıştır.

2. KAPSAM VE SORUMLULUKLAR

Bu politika elektronik veya fiziki ortamda GSO bilgi ve belgeleri ile bilgi sistem hizmeti erişimine izin verilmiş olan tüm çalışanları kapsamaktadır. Politika'nın uygulanması ve revizyonundan KVKK Komisyonu sorumludur. GSO nezdindeki tüm kullanıcılar, bu Politikada yer alan uygulamaları bilmek ve belirtilen kurallara uymakla yükümlüdür.

3. TANIMLAR

5651 sayılı Kanun	**İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**
6698 sayılı Kanun	6698 sayılı Kişisel Verilerin Korunması Kanunu
GSO/Kurum	Gaziantep Sanayi Odası
Güvenlik Duvarı (Firewall)	Güvenlik duvarı kurulduğu sisteme gelen ve giden ağ trafiğini kontrol ederek yetkisiz veya istenmeyen yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem
Özel Nitelikli Kişisel Veri	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri.

Politika	İşbu Kişisel Verilerin Korunması Uyum Süreci Politikası'nı
Sunucu (Server)	Bilgisayar ağlarında, diğer ağ bileşenlerinin (kullanıcıların) erişebileceği, kullanımına ve/veya paylaşımına açık kaynakları barındıran bilgisayar birimi.
Veri İşleyen	Veri sorumlusunun vermiş olduğu yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi
Veri Sahibi/İlgili Kişi	Kişisel verisi işlenen gerçek kişi
Veri Sorumlusu	Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi
VPN	Kurum dışında da Kurum ağına bağlanılmak üzere kullanılan sanal özel ağ.

4. İÇERİK

İşbu Politika kapsamında GSO nezdinde gerçekleştirilen faaliyetlerin 6698 sayılı Kanun'a uygun şekilde uygulanması amacıyla birçok prosedüre yer verilmiştir. İçerikte yer alan diğer politikalara ait dokümantasyon listesi EK-1 de yer almaktadır.

GSO nezdinde kullanılan bilgi ve haberleşme sistemleri ve donanımları (internet, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, taşınabilir cihazlar ve cep telefonları da dahil olmak üzere) GSO işlerinin yürütülmesi için kullanılmalıdır. Bu sistemlerin yasa dışı, rahatsız edici, GSO'nun diğer kural ve standartlarına aykırı veya GSO'ya zarar verecek herhangi bir şekilde kullanımı bu Politikanın ihlal edildiği anlamına gelecektir.

GSO, bu sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutmaktadır.

GSO nezdinde bulunan taraflar ile ihtiyaç ve beklentilerin hangi yöntem veya araç ile ortaya konulduğu, bu ihtiyaç ve beklentilerden hangilerinin uyum yükümlülüğü olduğu ve tarafların iletişim metodu aşağıdaki tabloda gösterilmiştir.

	İlgili taraflar	**İlgili taraf ile beklentilerin belirlendiği araç / yöntem**	**İletişim Metodu**
Birinci Taraflar	Çalışanlar	Kişisel verilerin korunması, görev ve talimatların belirlenmesi, sürekli eğitim ve etkinliklerin arttırılması, eğitim katılımlarının değerlendirilmesi, takdir, objektif ve şeffaf performans değerlendirmesi, mesai ve dinlenme saatlerine yasal uyumluluk, sağlıklı ve temiz bir çalışma ortamı	E-posta, telefon, yüz yüze görüşme, meclis toplantıları
	Üst Yönetim	Yasal ve mevzuat şartlarına tam uyum, TOBB ve Üyeler nezdinde örnek olma, çalışanların görev ve sorumluluklarına riayet edilmesi, politikalara uyum	

İkinci Taraflar	Üyeler	Üyelerin memnuniyetinin sağlanması, Sanayi Odası faaliyetlerinin aktif olarak takip edilmesi	Resmi yazışma, e-posta, telefon, yüz yüze görüşme, toplantılar
	Tedarikçiler	GSO çalışma alanlarının güvenliğinin sağlanması, GSO'nun taahhütlerine uyması, sürekli iletişim sağlanması, sağlıklı geri beslemelerin alınabilmesi, beklentilerin açık bir şekilde ifade edilmesi	
Üçüncü Taraflar	TOBB, Belgelendirme Kuruluşları, Diğer Odalar, Sektörle İlgili Ulusal ve Uluslararası STK'lar, Meslek Odaları, Resmi Makamlar, Diğer Paydaşlar	Yasal mevzuat şartlarına tam uyum sağlanması, her zaman insanı ve çevreyi korumaya yönelik faaliyetlerde bulunulması, GSO'nun taahhütlerine uyması, sürekli iletişim sağlanması	Resmi yazışma, e-posta, telefon, yüz yüze görüşme, toplantılar

5. UYGULAMA POLİTİKALARI

5.1. P.02. E-POSTA POLİTİKASI

Amaç

Kurum e-postalarının uygun olmayan kullanımı, Kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenemeyen sonuçlara neden olabilir. İşbu Politika, Kurum e-posta altyapısına yönelik kuralları ortaya koymaktadır. Kurumda oluşturulan e-postalar resmi bir kimlik taşımaktadır. E-posta, GSO'nun en önemli iletişim kanallarından birisidir ve gönderilecek tüm e-postalarda Kurum çalışanlarının işbu Politika ile belirtilen kurallara uyması gerekmektedir.

Kapsam

E-posta Politikası Kurum e-postasını kullanma yetkisi bulunan tüm çalışanları kapsamaktadır.

Politika

- Kurum e-posta kaynakları öncelikle Kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
- Kurum çalışanlarının Kurum e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar GSO'nun bilgi varlığıdır. Bu yüzden yetkili kişiler gerekli durumlarda önceden haber vermeksizin e-posta mesajlarını denetleyebilir veya yasal merciler ile paylaşabilir.
- Çalışanların e-posta adresi isim olacak şekilde açılmaktadır. Benzer isimlerin olması durumunda e-posta belirleme yöntemlerine göre kurulum işlemi gerçekleştirilir.
- Kurum e-posta kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
- Kullanıcılar kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur. Çalışan kendi kullanımı için verilen kullanıcı adını ve şifresini başkaları ile paylaşmamalı, kullanımı için başkasına vermemelidir.
- Kurumsal e-posta hesaplarının kişisel amaçlı kullanımı yasaktır.
- Kişisel kullanım için internet sitelerine üye olunması durumunda Kurum e-posta adreslerinin kullanılması yasaktır.
- Kurumun e-posta sistemi taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine veya Bilgi Güvenliği Ekibine haber verilmesi ve bu mesajın tamamen silinmesi gerekmektedir.
- E-postaların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

- Kurum dışına gönderilen tüm e-postalarda aşağıdaki uyarı mesajı bulunmalıdır.

"Bu e-posta ve ekleri gönderilen kişi veya kurum ile gönderildiği kişi veya kuruma ait özel, gizli veya yasak bilgiler içeriyor olabilir. İletinin yetkili muhatabı değilseniz e-posta içeriğinde yer alan gizli bilgileri ve kişisel verileri yetkisiz olarak elinizde bulundurmuş ve işlemiş kabul edileceğinizden iletiyi saklamayınız, kopyalamayınız, kullanmayınız veya iletmeyiniz. Mesajda yer alan bilgilerin üçüncü kişilere ifşa edilmesi etik kuralların ihlali anlamına geleceğinden mesajı ve ekleri gecikmeden yok ediniz, içindeki bilgileri kimseyle paylaşmayınız ve göndereni uyarınız. Gaziantep Sanayi Odası bu iletinin ve iletinin içeriğinde yer alan bilgi ve kişisel verilerin doğruluğu, bütünlüğü, iletilmesi ve benzeri hususlar konusunda garanti vermemektedir. İleti içeriğinde yer alan kişisel verilerin yetkisiz kullanımı ve işlenmesi sonucu Gaziantep Sanayi Odası'nın uğrayacağı her türlü zararı talep ve tazmin hakkı saklıdır. Gönderici, elektronik posta aktarımı sırasında meydana gelebilecek hata ve ihmallerden dolayı herhangi bir sorumluluk kabul etmemektedir. Kişisel Verilerin Korunması Kanunu kapsamında Aydınlatma Metinlerimize https://www.gso.org.tr/tr/genel-sayfa/sartlar-politikalar/kisisel-verilerin-korunmasi-kanunu-51.html *linkinden ulaşabilirsiniz."*

- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında derhal Bilgi Güvenliği Ekibine haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemelidir. Spam, zincir e-posta vb. zararlı e-postalara yanıt yazılması yasaktır.
- Kullanıcıların kullanıcı adı/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak herhangi bir işlem yapılmaksızın derhal Bilgi Güvenliği Ekibine haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Çalışanlar e-postalarını düzenli olarak kontrol etmeli, gelen e-postalara en geç 2 gün içerisinde cevap vermelidir.
- Çalışanlar, Kurum e-postalarının Kurum dışındaki kişiler ve yetkisiz kişilerce görülmesini engellemelidir.
- Kurumsal e-posta hesaplarına gelen e-postaların Kuruma ait olmayan kişisel e-posta hesaplarına yedeklemek veya bilgi amaçlı göndermek yasaktır.
- Kurum adı kullanılarak resmi iletişimlerde kullanılması amacıyla Hotmail, Gmail vb. mail hesaplarının açılması ve kullanılması yasaktır.
- Kurum e-posta kaynakları hiçbir şekilde yasa dışı kullanılamaz ve Kurum çıkarlarıyla çatışamaz, Kurumun normal operasyon ve iş aktivitelerini engelleyemez.
- Kurum e-posta kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.
- Kurumun e-posta sistemi taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
- Çalışanlar tarafından geçici veya sürekli haklara sahip olunması durumunda dahi e-posta yazılımının mevcut güvenlik ayarlarının değiştirilmesi yasaktır.
- Kullanıcılar e-posta yazılımının gönderenin kimliğini gizleyecek özelliklerini kullanamazlar.
- Kullanıcılar e-posta yazılımının otomatik mesaj iletme özelliklerini kullanamazlar.
- Kurum, e-posta sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar ve gerektiğinde bu hakkı kullanabilir.
- Kurum, kullanıcının e-posta sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar.

5.2. P.03. YAZILIM KULLANIM POLİTİKASI

Amaç

İşbu Politika, Kurum nezdinde kullanılan lisanlı yazılımların kullanım amaçlarının belirlenmesi amacıyla oluşturulmuş olup Kurum çalışanlarının işbu Politika ile belirtilen kurallara uyması gerekmektedir.

Kapsam

Yazılım Kullanım Politikası Kurum nezdinde mevcut olan herhangi bir yazılımı kullanan veya kullanma yetkisi bulunan tüm çalışanları kapsamaktadır.

Politika

- Kullanıcılar yazılımlarla ilgili tüm telif hakkı yasalarına uymak zorundadırlar.
- Kurum tarafından kullanılan tüm yazılımların lisansları yasal yollardan temin edilmiştir.
- Kuruma ait yazılımlar kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
- Kullanıcıların Bilgi Güvenliği Ekibinin izni olmaksızın mevcut yazılımlar dışında herhangi bir yazılımı yüklemesi veya kullanması yasaktır.
- Standart olarak Kurum bilgisayarlarında kurulan programlar aşağıda belirtilmiştir.

Eset-Google Chrome-Java- Adobe Acrobat Reader DC- Microsoft Office- Skype Desktop-Winrar-Winzip –Media Player

Standartta belirlenmeyen fakat iş yapma amacıyla ihtiyaç olunan yazılımların çalışanın birim yöneticisi onaylı e-posta yoluyla kurulum talep etmesi ardından Bilgi Güvenliği Ekibi tarafından yazılımın uygunluğu kontrol edilerek Kurum bilgisayarına yüklenir.

- Kuruma ait yazılımlar yasa dışı, Kurum politikalarına aykırı ve Kurum çıkarlarına ters düşecek şekilde kullanılamaz.
- Kuruma ait yazılımların izinsiz çoğaltılması ve kişisel amaçlarla kullanılması yasaktır.
- Kurum haberleşme alt yapısı ticari hiçbir yazılımın izinsiz kopyalanması, gönderilmesi, alınması veya çoğaltılması için kullanılamaz.
- Kurum, kullanıcı bilgisayarlarında yüklü bulunan veya kullanılan yazılımları herhangi bir zamanda kontrol edebilir.
- Kurum, kullanıcının yazılımlar üzerinden gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar ve gereken durumlarda bu hakkı kullanabilir.
- Kurum yetkili personelince tespit edilen ve lisans anlaşmalarına uymayan yazılımlar Bilgi Güvenliği Ekibi tarafından kaldırılır.

5.3. P.04. SUNUCU GÜVENLİK POLİTİKASI

Amaç

İşbu Politika, Kurumun sahip olduğu sunucuların temel güvenlik kurallarının belirlenmesi amacıyla oluşturulmuştur

Kapsam

Sunucu Güvenlik Politikası Kurumun sahip olduğu tüm sunucuları kapsamaktadır.

Politika

- Kurum bünyesinde bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.
- Sunucu işletim sistemleri üzerindeki kullanılmayan servisler ve uygulamalar kapatılmalıdır. Port açma talepleri Bilgi Güvenliği Ekibinin e-posta adresine mail olarak gönderilmeli ve yapılan talepte portun açık kalma süresi de beyan edilmelidir.
- Kullanılmayan sunucular güvenlik ve elektrik tasarrufu açısından kapalı tutulmalıdır.
- Sunucular üzerinde yapılan işlemlerin log kayıtları en az __ süre saklanacak şekilde ayarlanmalıdır.
- İşletim sistemleri, uygulamalar, veri tabanları, ağ donanımları yetkili erişim loğları tutulmalıdır.
- Sunucuların yönetimi için her yetkili kişi kendi hesabı ile bağlanarak işlem yapmalıdır, domainde olan sunucuların lokal admin hesapları kullanılmamalıdır.
- Sunuculara dışarıdan yapılan bağlantılar uzak bağlantı politikasının belirlediği kurallara göre yapılmalıdır.
- Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulmalıdır.
- Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenmelidir.

- Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt altına alınmalıdır. Sistem odalarına girişler çift güvenlik kontrolü ile yapılmalıdır.
- Sunucu odalarında ekipmanların bakımları düzenli olarak yapılmalı ve bakım kayıtları tutulmalıdır. Sistem odalarında cihazların bakımları yetkili kişiler gözetiminde yapılmalıdır.
- Elektrik ve data kabloları sunucu odaları dahil kurum içerisinde kanallardan geçmelidir.
- Sunucuların bulunduğu odalar kamera ile kayıt altına alınıp, gerektiğinde izlenebilir olmalıdır. Sunucuların bulunduğu odalara girişler sırasında kamera sistemi otomatik olarak mail ile yetkili kişilere fotoğraf göndermelidir.
- Elektrik kesintilerinden sistem odalarındaki sunucu ve diğer ekipmanların etkilenmemesi için UPS sistemine bağlı olması ve jeneratör ile desteklenmesi gerekmektedir.
- Sunucular yılda en az 2 kez zafiyet testinden geçirilmelidir.

5.4. P.05. MOBİL CİHAZLAR KULLANIM POLİTİKASI

Amaç

İşbu Politika GSO'ya ait bilgi içeren mobil cihazların kullanımı ile ilgili kuralların belirlenmesi amacıyla oluşturulmuştur.

Kapsam

Mobil Cihazlar Kullanım Politikası, GSO mobil cihazlarını kullanan tüm çalışanları kapsamaktadır.

Politika

- Kuruma ait bilgi içeren tüm taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.
- Kurum mobil cihazları öncelikli olarak Kurumun işlerinin gerçekleştirilmesi için kullanılmalıdır.
- Her çalışan kendisine zimmetlenen mobil cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
- Kullanıcıların mobil cihazlara erişim için şifre ya da parmak izi güvenlik sistemi kullanılmalıdır. Şifre konulması için çalışanlara gerekli bilgilendirme ve hatırlatmalar yapılmalıdır.
- Etki alanı dahilindeki bilgisayarlar admin yetkisi sınırlandırılarak yalnızca user yetkilendirmesi ile ilgili kişiye teslim edilmelidir. Etki alanında bağımsız olan bilgisayarların sorumluluğu çalışana aittir.
- Etki alanı dahilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar Kurum birimlerine ait ve yetki erişimi belirlenmiş olan ortak alanlara kaydedilmelidir.
- Mobil cihazların çalışanların aile bireyleri dahil zimmetlenen kişiler dışında kullanılması yasaktır.
- Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.
- Kurum mobil cihazlarının uygunsuz içeriği saklamak, erişmek, indirmek ve iletmek için kullanılması yasaktır.
- Kurum sabit telefonlarının kullanımı esnasında hoparlörler, ses ve video kayıt cihazları, video konferans ve benzeri cihazlar kullanılmadan önce görüşmede yer alan herkese bildirilmeli ve katılımcılardan izin alınmalıdır.
- Kuruma ait hassas bilginin yetkisiz kişilerin eline geçebileceği ortamlarda kullanıcılar bu bilgileri tartışmamalıdır.
- Çalışanların Kurum için gizli kabul edilebilecek belge ve dokümanları, ofis ortamında görünebilir yerlerde bırakması yasaktır. Yazıcı, faks veya fotokopi makinesinin kullanımlarında veri gizliliğine dikkat edilmelidir.
- Kurum, yazıcı ve faks cihazları kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
- Kurum, kullanıcının yazıcı ve faks cihazları ve Kuruma ait mobil cihazlar ile gerçekleştirdiği aktivitelerle ilgili bilgileri üçüncü partilere, emniyet birimlerine ve yargı makamlarıyla paylaşma hakkı saklıdır.

5.5. P.06. SABİT VE TAŞINABİLİR BİLGİSAYAR KULLANIM POLİTİKASI

Amaç

İşbu Politika, Kurum nezdinde çalışanlar tarafından kullanılan sabit ve taşınabilir bilgisayarların kullanımı ile ilgili kuralların belirlenmesi amacıyla oluşturulmuştur.

Kapsam

Sabit ve Taşınabilir Bilgisayar Kullanım Politikası Kurum nezdinde çalışan ve sabit ve taşınabilir bilgisayarları kullanım yetkisi bulunan tüm çalışanları kapsamaktadır.

Politika

- Kurum bilgi kaynaklarına uzaktan veya yerel ağ üzerinden erişmek için sadece Kurum envanterinde bulunan onaylanmış sabit ve taşınabilir bilgisayar cihazları kullanılmalıdır.
- Kuruma ait taşınabilir bilgi işleme cihazları öncelikli olarak Kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
- Taşınabilir bilgi işleme cihazları gözetimsiz bırakıldıklarında mutlaka fiziksel olarak güvenli bir yerde veya şekilde saklanmalıdır.
- Çalışanlar sabit ve taşınabilir bilgisayarları Kurum bünyesindeki domain'e bağlı olarak çalıştırmalıdır.
- Tüm bilgisayar sistemi yöneticisinin yetkisi altındadır. Sistem yöneticisi; tüm kullanıcı sistemlerine erişme, bilgisayar hesabının kontrol sahipliği, ihtiyaç olduğunda uzaktan erişim, sistem konfigürasyonunda değişiklik, sistem loğlarına erişim, yeni software/hardware kurulumu ve düzenlemesi yetkilerine sahiptir.
- Kurum çıkarlarıyla çakışmadığı sürece taşınabilir bilgisayarların kişisel kullanımına kısıtlı olarak izin verilebilecektir.
- Kurum bünyesinde çalışanlar, ofis ortamında veya dışında, sabit ve taşınabilir bilgisayarlarını terk ettikleri zaman kilitlemeli diğer kişi ve çalışanların izinsiz ve uygunsuz kullanımlarına izin vermemelidir.
- Bilgisayar üzerinde kişisel oturumlardan birinci derecede çalışanlar sorumludur.
- Bilgisayarlarda şifre korumalı ekran koruyucu aktif olmalıdır.
- Cihazların kullanımı esnasında ilgili yasa ve düzenlemelere uyulmalıdır.
- Kuruma ait taşınabilir bilgisayar cihazları hiçbir şekilde yasa dışı, Kurum çıkarlarıyla çatışabilecek veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanılamaz.
- Kurum bilgileri sabit ve taşınabilir bilgisayarlardan aksi belirtilmedikçe birim yöneticileri ve yönetim dışındaki çalışanlar tarafından taşınabilir medya aracılığıyla (USB, CD vb.) veri aktarımı yapılamaz. İş amaçlı özel kullanım taleplerinde ilgili birim yöneticisinin yazıl onayı olmak suretiyle diğer çalışanlara gerekli durumlarda bu yetki sadece o iş sürecinde verilebilmektedir.
- Her tür bilgi, zararlı yazılımlara karşı taramadan geçirilmeden Kurum ağına aktarılamaz.
- Kurum, sabit ve taşınabilir bilgisayarlar kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar ve gerektiğinde bu hakkını kullanabilir.
- Kurum kullanıcıların sabit ve taşınabilir bilgisayar cihazları ile gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar.

5.6. P.07. ŞİFRE POLİTİKASI

Amaç

İşbu Politika, Kurum nezdinde kullanılacak her türlü şifreleme sistemlerinin güvenli bir şekilde oluşturulması ve aynı düzeyde koruma sağlanması amacıyla oluşturulmuştur.

Kapsam

Şifre Politikası, Kurum nezdindeki bilgisayarları ve sunucuları kullanan tüm kullanıcı hesaplarını ve çalışanları kapsamaktadır.

Politika

- Şifreleme, bilgisayar ve hesap güvenliği için önemli bir özelliktir. Şifreler kompleks olmalıdır. Kolay tahmin edilen (memleket, çocuk, doğum tarihi, ardışık rakam ve harfler, İstanbul Ankara, Gaziantep, 1qaz2wsx, qwerty vb.) şifreler kullanılmamalıdır.
- Kurum içerisinde kullanılan genel kullanıcı bilgisayarları şifreleri 90 günde bir değiştirilmesi zorunlu kılınmıştır. Sistemler ile zorunluluk getirilmeyen hesapların şifreleri de 90 günde bir değiştirilmesi zorunludur.
- Üretim sürecinde kullanılan tüm bilgisayarların şifreleri 6 ayda bir değiştirilmesi zorunludur.
- Oluşturulacak şifre son 3 şifre ile aynı olamaz.
- Oluşturulacak şifre içerisinde Türkçe karakter bulunmamalıdır.
- Bilgisayar kullanıcı hesaplarının şifreleri en az 8 karakter olmalıdır. Kompleks şifre içeriğinde Büyük Harf, Küçük Harf, Rakam, Özel Karakter seçeneklerinden en az 3 tanesinin olması gerekmektedir.
- Kullanıcılar bilgisayar başından kalktığı zaman mutlaka oturumlarını kilitlemelidirler. (Windows +L) Genel kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 5 dakika içerisinde şifreli ekran korumasına girmelidir.
- Hatalı şifrelerin 10 defa üst üste denenmesi sonucunda kullanıcı hesabı otomatik olarak 20 dakika kilitlenecektir. Şifrelerin unutulması durumunda Bilgi Güvenliği Ekibi ile iletişime geçilmelidir.
- Kurumsal hesaplara ait şifrelerin e-posta iletilerine veya herhangi bir elektronik forma yazılması yasaktır.
- Şifrelerin aile bireyleri dahil herhangi bir üçüncü kişi ile paylaşılması, kağıtlara veya elektronik ortamlara yazılması yasaktır.
- Bilgi Güvenliği Ekibi tarafından oluşturulan geçici şifrelerin değiştirilmesi zorunludur.
- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de şifre kuralına göre belirlenmelidir.
- Uygulamalara, hesaplara veya bilgisayarlara giriş şifresinin unutulması veya herhangi bir sorun yaşanması durumunda derhal Bilgi Güvenliği Ekibine haber verilmelidir.
- Kurum, şifre ile kullanılan hesapları ve bilgisayarları izleme hakkını saklı tutar ve gerektiğinde bu hakkını kullanabilir.
- Kurum kullanıcıların şifre ile gerçekleştirdiği işlemlere ait bilgileri üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar.

5.7. P.08. FİZİKSEL GÜVENLİK POLİTİKASI

Amaç

İşbu Politika, Kurum personeli ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve Kurum binalarına yetkisiz girişlerin önlenmesi amacıyla oluşturulmuştur.

Kapsam

Fiziksel Güvenlik Politikası, Kurum binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını kapsamaktadır.

Politika

- Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları oluşturulmalıdır.
- Kurum dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi, yetkili görevliler gözetiminde gerçekleştirilmelidir.
- Tanımlanan farklı güvenlik bölgelerine erişim yetkileri düzenli aralıklar ile kontrol edilmelidir.
- Kurum girişleri, meclis toplantı salonları ve sistem odaları gibi kritik alanlar güvenlik açısından kamera ile kayıt altına alınmalıdır.

- Kritik sistemler özel sistem odalarında tutulmalıdır.
- Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karlı koruma altına alınmalıdır.
- Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.
- Kritik bilgi içeren idari alanlara kargo teslimatı yapılması yasaktır. Kargolar ilgili kişilere güvenlikte teslim edilmelidir.
- Ekipmanların kullanımı zimmetlenen kişiye aittir. Ekipmanların güvenliğinin sağlanması kişinin sorumluluğundadır. Teslim edilen ekipmanlara gelecek zararlar zimmet edilen kişiden tahsil edilecektir.
- Kurum içerisine giriş ve çıkışlar kamera sistemi ile kayıt altına alınmalıdır.

5.8. P.09. ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

Amaç

İşbu Politika, Kurum'un bilgi sistemlerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda uyulması gereken kuralları belirlemek amacıyla oluşturulmuştur.

Kapsam

Üçüncü Taraf Güvenlik Politikasının uygulanmasından Kurum birimlerinin tamamı sorumludur.

Politika

- Kuruma ait bilgi sistemlerinin veya bilgi varlıklarının bakımı, güncellenmesi vb. amaçlar ile işlem yapmak üzere Kuruma gelen tedarikçi, bakım firmaları veya üçüncü taraflar ile Gizlilik Sözleşmeleri yapılmalıdır.
- Üçüncü taraflar Kurum içerisinde bulundukları sürece Kurum politikalarına uygun hareket etmekle yükümlüdürler.
- Bilgi sistemlerinde veya bilgi varlıkları üzerinde yapılacak çalışmalar hakkında GSO Genel Sekreterliği ve Bilgi Güvenliği Ekibine bilgi verilmesi zorunludur.
- Bakım firmaları, tedarikçiler veya üçüncü taraflar Kurumun bilgi sistemlerine kendilerine verilen yetki kapsamında erişim sağlayabilirler.
- Bakım firmalarına, tedarikçilere veya üçüncü taraflara verilen erişim yetkileri, erişim amaçlarına uygun olacak şekilde kısıtlı verilmeli, loğları saklı tutulmalı ve çalışma bittikten sonra verilen yetkiler hemen geri alınmalıdır.
- Bakım firmaları, tedarikçiler veya üçüncü taraflar bilgi sistemlerine ve bilgi varlıklarına eriştikleri süre boyunca refakatçisiz bırakılmamalıdır.
- Kurum, işbu Politika ile düzenlenen kurallar üzerinde değişiklik yapma ve ek önlemler alma hakkını saklı tutar.

5.9. P.10. GİZLİLİK POLİTİKASI

Amaç

İşbu Politika, Kurum çalışanlarının sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarının belirlenmesi amacıyla hazırlanmıştır.

Kapsam

Gizlilik Politikası Kurum bünyesindeki tüm çalışanları kapsamaktadır.

Politika

- Kurumun gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimi dışında bu bilgilerin kopyalanması ve iletilmesi yasaktır.
- Kurum personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazların güvenliğini sağlamakla yükümlüdür. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.
- Hiçbir personel, bilgisayarındaki anti virüs koruma yazılımını devre dışı bırakamaz.

- Ortak alanlar üzerinde bulunan herkesin kullanımına açılmış olan “GENEL” klasörüne gizli ya da çok gizli bilgiler kopyalanmamalıdır. Bu alan üzerinde film, müzik gibi bilgiler paylaşılmamalıdır.
- Kullanıcı bir bilginin çok gizli olduğunu düşünüyorsa o bilgi şifrelenmeli veya yetkili kişiler dışında erişilemeyecek alanlarda saklanmalıdır.
- Bilgisayarlar üzerinden Kuruma ait dokümanlar haricinde dosya alışverişinde bulunulmamalıdır.
- Kritik veya gizli raporların dökümünü alan çalışan, rapor içeriğindeki bilginin uygun şekilde (kilitli dolap, çekmece vb.) korunmasından sorumludur.
- Herhangi bir kişi kendisine ait olmayan kritik bir rapor bulur ise bu durumu derhal Bilgi Güvenliği Ekibine bildirmelidir.
- Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez. Saatler sistem tarafından otomatik olarak yönetilmektedir.
- Taşınabilir bilgisayarlar güvenlik açıklarına karşı daha dikkatli korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda hemen Bilgi Güvenliği Ekibine bildirilmelidir.
- Kurum bünyesinde edinilmiş olan ticari sır, patent, üretim, üye bilgileri kesinlikle yetkisiz kişiler ile paylaşılmamalıdır.
- Kurum bilgisayarlarında kişisel verilerin barındırılması yasaktır. Kuruma ait cihazlarda tutulan ve iletilen tüm bilgiler Kurum malıdır ve Kurum bu bilgileri izleme ve denetleme hakkına sahiptir.
- Hiçbir çalışan, izin almadan kendi bilgisayarından veya başka bir kaynak kullanarak Kurumun bilişim ağını tarayamaz, izleyemez veya dinleyemez.
- Hiçbir çalışan, Kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.
- Sosyal medya erişim izni verilen çalışanların görevlerinin dışında bu hesapları kullanmaları yasaktır.
- Sosyal medya üzerinden Kurumu rencide edici, karalayıcı paylaşımlar yapılmamalıdır. Kurumun hassas bilgileri sosyal medya üzerinden paylaşılamaz.
- Kuruma ait bilgisayar, telefon, yazıcı, faks, fotokopi, tarayıcı vb. donanımlar şahsi işlemler için kullanılmamalıdır. Bilgisayar, telefon, yazıcı, faks, fotokopi, tarayıcı vb. cihazlarda şahsi kullanım tespit edildiğinde Kurumun İnsan Kaynakları Direktörlüğüne bilgi verilecektir.
- Kurum envanterinde kayıtlı olmayan kişisel bilgisayar ve cep telefonu gibi cihazların bakım onarımı için Bilgi Güvenliği Ekibine başvuru yapılması gerekmektedir.
- Kurum, işbu Politikanın uygulanırlığının denetimi amacıyla kullanıcıların sahip olduğu tüm varlıkları izleme yetkisini saklı tutar.
- Kurum, kullanıcılar tarafından işbu Politika kapsamında gerçekleştirilen işlemleri izleme yetkisi kapsamında elde edeceği bilgileri üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar.

5.10. P.11. TEMİZ MASA TEMİZ EKRAN POLİTİKASI

Amaç

İşbu Politika, GSO bünyesindeki kağıtlar, taşınabilir depolama ortamları ve kişisel vilgisayar için mesai saatleri içinde ve dışında bilgiye yetkisiz erişim ve bilginin hasar görmesi gibi riskleri azaltmak için gerekli olan şartların oluşturulması amacıyla hazırlanmıştır.

Kapsam

Temiz Masa Temiz Ekran Politikası GSO bünyesindeki tüm çalışanları kapsamaktadır.

Politika

- Kuruma ait uygulamalarda kullanılan şifreler iş arkadaşları da dahil olmak üzere kimse ile paylaşılamaz. Şifrelerin yazılı olarak post-it ya da not kağıtlarına yazılarak pano, bilgisayar ekranı, klavye gibi donanımlara yapıştırılamaz.

- Evrak ve dokümanların güvenliği için çalışma saatleri dışında ofis kapılarının kilitli tutulması gerekmektedir.
- Evrak ve dokümanlarda yer alan bilgilerin farklı kişiler tarafından ele geçirilmemesi için klasörlerde saklanmalıdır.
- Hassas bilgi içeren evrak klasörleri ve Kuruma ait başlıklı kağıtlar kilitli dolaplarda saklanmalıdır.
- Kağıtların doğrudan çöp kutusuna atılması yasaktır. İmha edilecek kağıtlar kağıtlar için kağıt kırpma makinesi kullanılmalıdır.
- Hassas ve kritik bilgi içeren evraklar ağ üzerinden paylaşılamaz.
- Masa üstü doküman sayısını artırmamak için mümkün olduğu kadar elektronik dokümanların yazıcıdan çıktılarının alınmamasına dikkat edilmelidir.
- Masa üzerinde kartvizit kutuları, kişisel ajandalar, değerli bilgilere sahip dokümanlar bırakılamaz ve bunlar kilitli çekmecelerde muhafaza edilmelidir.
- Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.
- Kuruma ait kritik bilgi içeren dokümanlar başkaları tarafından farkedilmeyecek şekilde muhafaza edilmelidir.
- Çalışanların kişisel gizli bilgileri (maaş bordrosu vb.) başkaları tarafından farkedilmeyecek şekilde muhafaza edilmelidir.
- Çalışanlar telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranmakla yükümlüdür.
- Bilgi ve veri alışverişinden önce dış tarafların kimlikleri tespit edilmelidir.
- Kurum bünyesinde kullanılan toplantı salonlarında gizli ve kritik bilgi içeren dokümanları toplantı sonrasında ilgili salonlarda bırakmamalı ve salonlardaki tahtalara alınan notlar silinmelidir.
- Gizlilik içeren bilgilerin umumi yerlerde konuşulması yasaktır.
- Gizlilik içeren bilgiler telefonlarda ses dışarıya açık olarak görüşülmemelidir. Faks yoluyla gizlilik içeren herhangi bir bilgi gönderilmemelidir.
- Bilgisayar gibi elektronik ortamlarda bulunan bilginin korunması için çalışma saatleri dışında da ofis kapıları kilitli tutulmalıdır.
- Kısa süreli ayrılmalarda dahi, cep telefonu, taşınabilir bellek, harici hard disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.
- Bilgisayarlar gözetimsiz bırakıldığında kapatılmalı veya parola kullanılarak korunmalıdır. Ekran koruyucu aktif hale getirilmelidir. Bu işlem Windows bilgisayarlarda Windows +L, Mac bilgisayarlarda Control+Shift+Eject tuşlarına basılarak kolayca yapılabilmektedir.
- Bilgisayarların masaüstlerindeki klasör ve dosyalar düzenli şekilde tutulmalıdır.
- Fotokopi cihazlarının yetkisiz kullanımı önlenmelidir.
- Fotokopi cihazlarının belleğinde bulunan kritik ve hassas bilgiler silinmelidir.
- Hassas ve sınıflandırılmış bilgi içeren ortamlardaki bilgiler yazıcıdan çıktı alındıktan sonra hemen silinmelidir.
- Şifreler yazılı olarak saklanmamalı ve hassas bilgiler silinmelidir.
- Kullanılan şifreler tahmin edilebilir olmamalıdır. Şifreyi oluşturan kişi ile ilgili bilgiler içermemelidir. Ardışık, tümü sayısal ya da tümü alfabetik karakterlerden oluşmamalıdır.
- Çalışanlara kendilerine ait bilgisayarlarda, taşınabilir belleklerde, harici diskte ve benzeri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi ve belgelerin güvenliğini sağlamakla yükümlüdür. Taşınabilir bellek veya harici diske gizli, önemli veya özel nitelikli kişisel veri konulması gerekiyor ise kriptolayarak korunması gerekmektedir.
- Gizli belgelerin, şifrelerini adreslerin, özellikle taşınabilir bellek, e-posta, sosyal medya gibi alanlarda paylaşılmamasına dikkat edilmelidir.
- Bilinmeyen e-posta ve haber gruplarına üye olunmamalıdır.

- Elektronik posta ortamında kişisel şifre bilgileri paylaşılmamalıdır.
- Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımından sonra etki yöntemler kullanılarak geri dönülmeyecek şekilde silinmesi gerekmektedir.
- Kuruma ait yürütülen iş ve işlemlerde Kuruma ait e-posta adreslerinin kullanılması zorunludur.
- Kurumsal işlerin yapıldığı bilgisayarlar çalışanın kendi sorumluluğundadır. Kurum bilgisayarlarının çalışan haricinde yetkisiz kullanıcılara teslim edilmesi yasaktır.

5.11. P.12. KRİPTOGRAFİK KONTROLLER POLİTİKASI

Amaç

İşbu Politika, bilginin gizliliği, erişilebilirliği veya bütünlüğünün korunması amacıyla oluşturulmuştur.

Kapsam

Kriptografik Kontroller Politikası, kritik bililerin güvenli erişimi ve paylaşımı amacıyla tüm Kurum çalışanlarını kapsamaktadır.

Politika

- Kurum içerisinde tanımlanan gizli bilgi varlıkları ve özel nitelikli kişisel veriler kriptografik şifreleme yöntemleri ile saklanmalıdır. Her çalışan kendi barındırdığı bilgi varlıklarının ve özel nitelikli kişisel verilerin güvenliğinden sorumludur.
- Kurumlar arası bilgi alışverişlerinde ve özellikle kamu kurumları ile yapılan yazışmalarda e-imza, mali mühür gibi sistemler kullanılarak veri transferi yapılmalıdır.
- Kurum sistemlerine dışarıdan yapılacak her türlü uzak bağlantı SSL VPN sistemi üzerinden yapılmalıdır.
- Mobil cihazlardaki verilerin korunmasında güçlü şifre kullanılmalıdır.
- Kurum, Kriptografik verilerin paylaşımını ve saklanmasını izleme hakkını saklı tutar ve gerektiğinde bu hakkını kullanabilir.

5.12. P.13. KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

Amaç

İşbu Politika, Kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarının belirlenmesi amacıyla oluşturulmuştur.

Kapsam

Kurumun bilgi sistemlerine erişim Kurum çalışanları ile Kurum dışı kullanıcılar Kimlik Doğrulama ve Yetkilendirme Politikası kapsamındadır.

Politika

- Kurum sistemlerine erişecek tüm kullanıcıların bilgisayar erişim hesapları doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.
- Kurum sistemlerine erişmesi gereken tedarikçilere veya üçüncü kişilere yönelik kullanıcı hesabı Bilgi Güvenliği Ekibi tarafından ilgili yetkiler verilerek tanımlanacaktır.
- Kurum bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri üzerindeki kullanıcı yetkileri belirlenmeli ve denetim altında tutulmalıdır.
- Çalışanlara ve üçüncü kişilere verilen erişim yetkilerinin güncelliği sağlanmalıdır.
- İşletim sistemleri üzerindeki erişim loğları düzenli olarak tutulmalı, gerektiği durumlarda kontrol edilebilmelidir.
- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
- Erişim gereksinimi artık kalmamış kullanıcıların hesapları Bilgi Güvenliği Ekibi tarafından pasif duruma alınmalı veya kaldırılmalıdır.
- Kurum, kendi inisiyatifi doğrultusunda erişim yetkilerini belirleme, pasife alma veya kaldırma yetkisini saklı tutar.

6. UYGULAMA VE YAPTIRIM

Kurum çalışanlarının işbu Politika kapsamında yer alan politikalara ve Kuruma ait diğer politika ve prosedürlere aykırı kasti veya kasıtsız davranışları hakkında Bilgi Güvenliği Disiplin Prosedürü uygulanacaktır. Kurumun İş Kanunu, iş sözleşmeleri ve sair mevzuat hükümleri kapsamında yaptırım uygulama ve zararlarının tazmini için rücu etme hakkı saklıdır.

7.REVİZYON KAPSAMI

İlk yayındır.

HAZIRLAYAN	ONAYLAYAN
KVKK KOMİTESİ – BİLGİ İŞLEM DAİRESİ	GENEL SEKRETER