

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

AMAÇ

Amasya İl Özel İdaresi tarafından sağlanan bilgi teknolojileri, iletişim, bilişim, haberleşme ve internet hizmetlerini oluşturulan bilişim-iletişim-haberleşme araçlarının veri güvenliği mevzuat ve standartlarına uygun kullanımının sağlanması.

KAPSAM

Kabul Edilebilir Kullanım Politikası, Amasya İl Özel İdaresi varlık envanterinde bulunan;

- Kişisel bilgisayar,
- Sunucular,
- Uygulamalar,
- Kablolu/kablosuz bağlantılar,
- Tablet, dahili telefon, cep telefonu,
- Fotoğraf makinesi, kamera sistemi
- Hafıza çubuğu, disk, CD, disket v.b.
- Yazıcılar,
- Kişisel veya ortak kullanımda olan bilişim ve iletişim cihazları,
- E-Posta,
- İnternet hizmeti,
- Dosya ve bilgi paylaşım hizmetleri vb.
- Kullanımı ile ilgili olarak kurum çalışanlarının, kuruma iş yapan tedarikçilerin ve diğer paydaşların kurum varlıklarını nasıl kullanması gerektiği gibi kuralları kapsar.

UYGULAMA

Amasya İl Özel İdaresi tarafından sağlanan bilgi teknolojileri, iletişim sistemleri envanteri hiçbir şekilde Türkiye Cumhuriyeti yasalarına ve kurum içi yönetmeliklere, kurum kültürüne ve iş ahlakına aykırı faaliyetlerde bulunmak amacıyla kullanamaz. Amasya İl Özel İdaresi iş kanunu ve çeşitli iş ve işlemler için verilmiş olan kişisel veriler ve özel nitelikli kişisel verileri sadece iş amacıyla, kısıtlı ve yasalara uygun kullanılmasına izin verir. Tüm kullanıcılar bu duruma göre çalışmayı taahhüt ederler. Çalışanlar, tedarikçiler, yükleniciler iş ilişkisi sona erse de kurumumuza ait kişisel verileri Kurumumuzun yazılı izni olmaksızın paylaşamaz. Çalışanlar veri sorumlusu olan Üniversitemizin kurumsal e-postaları denetleyeceğini bilmelidir. Üniversite operasyonlarının güvenliği ve iş kontrolü için e-postaları denetleyebilir/denetletebilir. Bu nedenle kurumsal e-postalar şahsi işler için kullanılmamalıdır.

Kullanıcı Kimliğinin Belirlenmesi

Kullanıcılar bilgi sistemleri üzerinde kendilerine ait olmayan veya gizlenmiş kullanıcı kimliklerini kullanamazlar. Kullanıcılar zorunlu durumlar dışında ortak hesap kullanımından kaçınmalıdır.

Şifre Parola Kriterlerinin Oluşturulması

Kurumdaki şifre parola Politikasına uyulmalıdır. Bilgi sistemleri teknik olarak mümkün olan durumlarda parola karmaşıklık ve değişiklik kontrollerini teknik olarak uygulayacak biçimde yapılandırılır. Karmaşıklık ve değişiklik kontrolleri uygulanmadığı durumlarda kullanıcılar güçlü bir şifre seçimi yapması sağlanır. Kullanıcılar parola kriterlerinin teknik olarak

KVKK VERİ SORUMLUSU İRTİBAT KİŞİSİ	ONAY	FORM NO	P.KVKK.04
		YAYIM TARİHİ	02.01.2024
		REVİZYON NO	
		REVİZYON TARİHİ	
KVKK Belgesinin güncel hali için Amasya İl Özel İdaresi ağına bakınız			

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

zorlanmasının mümkün olmadığı durumlarda periyodu belirlenmiş hatırlatmalar gerçekleştirildiğinde parolalarını değiştirmekle yükümlüdür. Kurum e-postaları için kullanılan parolalar özel e-postalar için kullanılamaz.

Kurumsal Bilgi Paylaşımı

Amasya İl Özel İdaresi içi bilgi paylaşımı sadece görev gereği ilgili veriye ulaşması gereken kullanıcılar arasında olur. Kolluk kuvvetleri ve kamu kurumları ile bilgi paylaşımı gerektiği durumlarda bu irtibat Genel Sekreterlik veya İlgili müdürlük tarafından gerçekleştirilir. Kurumsal İnternet sitesinden yapılan yayınlar, yapılacak paylaşımlar, halka aktarılacak bilgiler, aktarılan verinin sınıflandırılması da göz önüne alınmak kaydı ile sadece İlgili müdürlük onayı ile yapılabilir.

Verilerin Sınıflandırılması ve Veri Sahipliği

Amasya İl Özel İdaresi çalışanları sorumlu oldukları bilgi varlıklarından ve bu verilerin korunmasından bizzat sorumludurlar. Veri sahipleri kendileriyle ilgili iş verilerinin sınıflandırılmasından ve gerektiğinde yeniden sınıflandırılmasından sorumludur.

Amasya İl Özel İdaresi Verilerinin Saklanması

Amasya İl Özel İdaresi'nde veriler saklama süreleri kadar bilgisayarlarda, çalışma ofislerinde ve kurum arşivinde saklanıp yasal saklama süreleri sona eren veriler ilgili mevzuat gereği imha edilir. Kurumda kişisel bilgisayar kullanılamaz ve kişisel bilgisayarlarda veri saklanamaz. Yapılan saklama, imha, anonimleştirme iş ve işlemleri Devlet Arşiv Hizmetleri Hakkındaki Yönetmeliğe uygun olmalıdır.

Temiz Masa, Temiz Ekran Politikası' na Uyum

Kullanıcılar kurumda kullanılmakta olan Temiz Masa Temiz Ekran Politikası' na uyumlu çalışmalıdırlar. Kullanıcılar masaları başında olmadıklarında hassas bilgi içeren basılı dokümanları masa üstünde bırakarak ve bilgisayar ekranlarını açık bırakarak terk etmemelidir. Hassas/kritik bilgi içeren basılı dokümanlar kullanılmadıklarında masadan kaldırılmalı ve gerekiyorsa kilit altında tutulmalıdır. Kullanıcılar Kurum dışında basılı doküman, bilgisayarlar ve veri saklama cihazlarının fiziksel güvenliği konusunda daha hassas davranmalı, asla kontrolsüz biçimde açıkta bırakmamalıdır. Çalışmaya ara verildiğinde veya ekran başından kalkındığında Windows + L tuşu ile veya başka bir şekilde ekran kilitlemelidir.

Kurumsal İletişimde Telefon Görüşmeleri

Çalışanlar özellikle kurum dışında hassas bilgileri içeren telefon görüşmesi yapmamaya gayret etmelidir. Hassas bilgilerin paylaşılması gerekiyor ise odanın kapısının kapalı olması, etrafta gizli bilgiyi duyacak kimselerin olmadığından emin olunması gerekmektedir. Kurumsal gizliliğe dikkat edilmelidir. Bu hususta 13.05.1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar" ın yerine 25.04.2022 tarihli ve 5529 sayılı Cumhurbaşkanı Kararıyla "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" e uygun hareket edilmelidir.

Taşınabilir Bilgisayar Kullanım Kuralları

KVKK VERİ SORUMLUSU İRTİBAT KİŞİSİ	ONAY	FORM NO	P.KVKK.04
		YAYIM TARİHİ	02.01.2024
		REVİZYON NO	
		REVİZYON TARİHİ	
KVKK Belgesinin güncel hali için Amasya İl Özel İdaresi ağına bakınız			

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Taşınabilir bilgisayarlarda tüm Hassas ve Gizli bilgiler şifreli olarak tutulmalıdır. Taşınabilir bilgisayarlar, kullanılmak üzere bir başka kişiye verilmemelidir. Taşınabilir bilgisayarlar üzerinden Kurum dışındaki kablosuz ağlara bağlanmak gereği olduğunda, kablosuz ağın güvenli ve kilitli bir ağ olup olmadığı kontrol edilecek, değilse bu bağlantı gerçekleştirilmeyecektir.

Taşınabilir Veri Saklama Araçları Kullanım Kuralları

Taşınabilir olmaları nedeniyle çalınma tehdidiyle karşı karşıya olan taşınabilir veri saklama araçlarının, özellikle kritik veri barındırmaları durumunda, fiziksel güvenliği kullanıcılar tarafından sağlanmalıdır. Verinin saklanma ihtiyacı sona erdiğinde veriler saklama cihazından geri dönüşümü olmayacak şekilde silinmelidir.

Kurum Ağına Erişim Kuralları

Ağa uzaktan erişim için, sıra dışı bir neden yoksa Kurum bilgisayarları kullanılmalıdır. Kullanıcılar uzaktan erişim araçlarını koruma konusunda diğer erişim araçlarının korunmasına nazaran daha üstün hassasiyet göstermelidir. Kullanıcılar Kurum bilgisayarı dışında bir bilgisayar kullanmak zorunda olduklarında, kullanılan bilgisayarın kişisel koruma duvarının olması, anti-virüs imzalarının ve işletim sisteminin güncel olması gibi kontrollere dikkat etmelidirler. Hiçbir personel izin almadan kendi PC' sinden veya başka bir kaynak kullanarak, Kurum ağını tarayamaz, izleyemez veya dinleyemez.

Kurumsal ve Kişisel Bilgilerin İnternet Üzerindeki Web Sitelerine Verilmesi

Kullanıcılar İnternet üzerindeki tartışma gruplarına, sohbet odalarına ve diğer forumlara yazmaları durumunda kurumun ve şahıslarının mahremiyetini korumalı, kurum adres ve telefon bilgilerini, personel isimlerini, unvanlarını, e-posta adreslerini ve diğer kişisel bilgilerini iş gerekleri ve kanuni gereklilikler dışındaki durumlarda İnternet üzerindeki herhangi bir web sitesine aktarmamalıdır.

İnternette Dosya İndirme

Çalışanlar, yönetim tarafından özellikle onay verilmesi dışındaki durumlarda İnternette yazılım indirilemez. Kullanıcılar iş gereksinimleri için izni veya yetkili olmaları durumunda İnternette veri dosyaları indirebilir, ancak anti-virüs imzaları ve işletim sistemi yamalarının güncelliğinden emin olmalıdır.

Mesajlaşma ve İletişim Mahremiyetinin Sağlanması

Bilgi sistemleri kullanılarak yapılan hiçbir elektronik iletişimin mahrem olacağı garantisizdir. Kullanıcılar elektronik ortamdaki her türlü iletişimlerinin (telefon iletişimi dâhil), kullanılan teknolojiye özgü saldırı yöntemleri ile hedeflenen alıcıdan farklı alıcılara yönlendirilebilme, iletişim içeriğinin izlenebilme ve saklanabilme risklerine tabi olduğunu bilmelidir. İş amaçlı kullanılacak mesajlaşma çözümü Kurum e-postasıdır. Yabancı sosyal medya iletişim şirketlerine kurumsal veri aktarmak sakıncalıdır. Sosyal medya iletişimi ancak şahsen kişisel işler için yapılabilecektir. Kurumsal mesajlaşma çözümlerinin yerli olması gerekmektedir.

Mesaj Ekleri Politikası, İstenmeyen e-postalar (SPAM), Phishing Saldırıları

KVKK VERİ SORUMLUSU İRTİBAT KİŞİSİ	ONAY	FORM NO	P.KVKK.04
		YAYIM TARİHİ	02.01.2024
		REVİZYON NO	
		REVİZYON TARİHİ	
KVKK Belgesinin güncel hali için Amasya İl Özel İdaresi ağına bakınız			

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Çalışanlar e-posta güvenliğinden bizzat kendileri de sorumludur. E-posta içinde gelen linklere tıklamamalıdır. Şüpheli e-postalardaki resimleri görüntülemek için indirmemeli, e-posta içindeki herhangi bir linke tıklamamalıdır. Çalışanlar şüphelendikleri durumları bilgi işlem birimine iletmelidir.

Tarayıcı, Faks, Yazıcılar ve Fotokopi Makinalarının Doğru Kullanımı

Çalışanlar gizlilik gereksinimi yüksek bir dokümanı yazdırırken, tararken, faks çekerken bilginin yetkisi olmayan kişiler tarafından görülmesini veya ele geçirilmesini engellemek için gereken gizliliği ve güvenliği sağlamakla sorumludur. Fotokopi makinalarında gizli bilgi içeren bilgi ve belgeler bırakılmamalıdır.

İhtiyaç Kalmayan Basılı Dokümanların İmha Edilmesi

İmha edilecek tüm hassas dokümanlar (gizli, özel ve hizmete özel bilgi sınıfında bulunan dokümanlar) ilgili mevzuata uygun olacak şekilde geri dönüşü olmayacak şekilde imha edilmelidir. Bu hususta 13.05.1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar" ın yerine 25.04.2022 tarihli ve 5529 sayılı Cumhurbaşkanı Kararıyla "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" e uygun hareket edilmelidir.

Güvenlik Olayları ve Gözlenen Zayıflıkların Bildirilme Sorumluluğu

Kullanıcılar kendi sorumluluk alanlarında gerçekleşebilecek veya diğer alanlarda gözlemleyebilecekleri güvenlik olay ve zayıflıklarına karşı duyarlı olmalıdır. Fark edilen her zayıflık, riskin gerçekleşmesi zayıf bir olasılık olsa bile en kısa zamanda BGYS Temsilcisine raporlanmalıdır.

İşlem Bilgisi ve Kayıtların Saklanması

Kurumda yapılan bilgi işlem faaliyetleri 5651 sayılı yasaya göre takip edilmelidir. Log kayıtları müdahaleye yer vermeyecek şekilde tutulmalıdır. Log kayıtlarının tutulması çalışanların işlem bilgilerinin takibi konusunda son derece önemlidir. Çalışanların bilgi sistemleri üzerinde veya bilgi sistemlerini kullanarak yasal mevzuata veya kurum içi kurallara aykırı davranışlarından şüphe edilmesi halinde üst yönetimin resmen talebi üzerine bilgi sistemleri üzerindeki faaliyetlerinin izlenebilecektir.

Kaynakların Yasalara ve Ahlak Prensiplerine Uygun Kullanımı

Personel, İnternet kullanımı ve sesli iletişim aktiviteleri dâhil olmak üzere, tüm bilgi sistemleri ve iletişim imkânlarının kullanım ve sağlanmasında, ilgili yasalara, uluslararası hukuka ve genel ahlak kurallarına uymakla yükümlüdür. Telif hakları yasaları ihlal edilemez

Yazılım Kurulumu Kuralları

İş ile ilgili olmayan yazılımların (kurulum dosyaları dâhil) bilgisayar sistemlerinde saklanması veya kurulması her koşulda yasaktır. Kullanıcılar, teknik olarak mümkün olsa bile, telif hakları kanunlarının çiğnenmesine ve teknik sorunlara neden olabileceğinden Yönetimin onayı olmadan bilgisayarlarına yazılım yüklemeyiz. İş amaçlı yazılım yükleme ihtiyacı olması durumunda Yönetimin görüşü ve onayı alınmalıdır. Yazılım kurulumu esnasında telif hakları yasaları ihlal edilemez.

KVKK VERİ SORUMLUSU İRTİBAT KİŞİSİ	ONAY	FORM NO	P.KVKK.04
		YAYIM TARİHİ	02.01.2024
		REVİZYON NO	
		REVİZYON TARİHİ	

KVKK Belgesinin güncel hali için Amasya İl Özel İdaresi ağına bakınız

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Yama Yönetimi, Konfigürasyon ve Güvenlik Ayarları

Çalışanlar programların yamaları ile ilgili bilgi işlem biriminin haberi olmadan inisiyatif kullanarak işlem yapamaz. Bilgisayarın güvenlik düzeyini düşürülemez. Konfigürasyon ve güvenlik ayar değişiklikleri sadece teknik personel tarafından ve gerekli olan süre için yapılabilir.

Bilişim ve İletişim Teçhizatlarının Fiziksel Güvenliğinin Sağlanması

Çalışanlar kendilerine tahsis edilmiş olan iletişim ve bilişim sistemlerini, mobil ve elektronik cihazları en iyi şekilde korumakla yükümlüdür. Çalışanlar iş yaparken sıvıları, yiyecek içecekleri bilgisayar ve ofis araçlarından uzak tutmalıdır.

Bilgi Güvenliği ve Gizlilik Esasları

Bu hususta 13.05.1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkında Esaslar" ın yerine 25.04.2022 tarihli ve 5529 sayılı Cumhurbaşkanı Kararıyla "Gizlilik Dereceli Belgelerde Uygulanacak Usul ve Esaslar Hakkında Yönetmelik" e uygun hareket edilmelidir. Kurumsal bilgiler ve gizlilik kapsamına giren bilgiler ilgili çalışan işten ayrılması durumunda dahi paylaşılmaz.

Yasalara Uyumun Sağlanması

Çalışanlar Bilgi Güvenliği Yönetim Sistemi (BGYS) ve KVKK Kişisel Veri Güvenliği Yönetim Sistemi (KVYS) kurallarını okumak ve uygulamakla yükümlüdür. Çalışanlar veri güvenliği ile ilgili T.C. kanunlarına, mevzuatlarına ve ikincil düzenlemelere uymakla yükümlüdür.

SORUMLULUKLAR

Bu politikanın uygulanmasından tüm çalışanlar ve bilgi varlıklarına erişim izin verilmiş olan Tedarikçi/yüklenici firma çalışanları sorumludur.

YAPTIRIM

Çalışanlar bilgi Güvenliği Yönetim Sistemi (BGYS) ve Kişisel veri güvenliği Yönetim Sistemi (KVYS) dokümanlarını DUYURU panoları üzerinden veya hizmetine açık ortak klasör olan "BGYS-KVYS" klasörü üzerinde okumak ve gereğini yerine getirmekle yükümlüdür. Bu politikaya uygun olarak çalışmayan tüm personel hakkında bu politika gereği disiplin işlemi uygulanır. Kabul Edilebilir Kullanım Politikası' na uymayan, uygunsuz kullanımın yoğunluğuna, verilen zararın boyutuna ve tekrarına göre disiplin kurallarının uygulanmasını kabul eder. Bu disiplin kuralları uyarı, kınama, işten çıkarma şeklinde olabilir. Gerekli hallerde kullanıcı erişimi sınırlı veya sınırsız süre ile kısıtlanabilir veya engellenebilir. Uygunsuzluğun durumuna göre adli yargı mekanizmaları harekete geçirilebilir. Kullanıcı, yasal ve teknolojik gelişmeleri göz önünde bulundurarak bu Kabul Edilebilir Kullanım Politikası' nın kısmen değiştirilebileceğinden haberdardır ve bunu açıkça kabul eder. Çalışan Kabul Edilebilir Kullanım Politikası' nı anladığını, tanıdığını ve Kabul Edilebilir Kullanım Politikası' na uyacağını kabul ve beyan eder.

KVKK VERİ SORUMLUSU İRTİBAT KİŞİSİ	ONAY	FORM NO	P.KVKK.04
		YAYIM TARİHİ	02.01.2024
		REVİZYON NO	
		REVİZYON TARİHİ	
KVKK Belgesinin güncel hali için Amasya İl Özel İdaresi ağına bakınız			