ANKARA SERBEST MUHASEBECİ MALİ MÜŞAVİRLER ODASI

BİLGİ GÜVENLİĞİ POLİTİKASI

Güncelleme Tarihi : 10/11/2021

1. AMAÇ VE KAPSAM

Bu Politikanın amacı, **Ankara SMMMO** (ya da "**Oda**") veri güvenliğinin sağlanması ve kişisel verilerin korunmasıdır. Bilgi Güvenliği Politikası, Gizlilik Politikasında tanımlanan politika hiyerarşisinin bir parçasıdır ve Gizlilik Politikası ile uyumlu olmak zorundadır. Bu politikada yapılacak değişikliklerle ilgili gerektiğinde Gizlilik Politikasında da düzeltmeler yapılır.

Politika, Yönetimin kararı ile yürürlüğe girer. Politika'nın uygulanması ise Yönetim tarafından görevlendirilen **Komite** tarafından takip edilir. **Oda** gerekli gördüğü durumlarda Politika'yı güncelleyebilir ve üzerinde değişiklikler yapabilir.

Oda, bu Politika ile kişisel verilerin elde edilmesi, işlenmesi, aktarılması ve silinme/yok edilmesine ilişkin her aşamada hukuka uygun bir şekilde hareket edilmesini amaçlamaktadır. **Oda** mevcut hukuk kuralları ile düzenlenmemiş konularda ise kişi yararını ön plana çıkarmayı amaçlar ve boşlukları doldururken bu yönde kararlar alır.

Bu politika, **Oda** bilgi işlem altyapısını kullanmakta olan tüm birimleri kapsamaktadır. **Oda**, bu politika ile iş faaliyetlerinin en az kesinti ile duraksamadan devam etmesini sağlamak için bilgi işlem hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziki ve dijital bilgi varlıklarının ve kişisel verilerin güvenliğini sağlamayı hedefler.

2. TANIM

Bilgi Güvenliği ve Gizlilik Politikası; **Oda** amaçlarına uygun düşecek nitelikte bilgi güvenliği politikası amaçları belirleyerek politikanın uygulanabilirliğine dair taahhütlerde bulunur ve bilgi güvenliğinin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve bilginin risk ve tehditlerden korunmasını sağlar.

3. İLKELER

Bilgi güvenliği kavramı aşağıdaki üç temel prensibi esas almak durumundadır:

3.1. Gizlilik

Bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

3.2. Bütünlük

Bütünlük, bilginin, kasten veya ihmal ile yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı, içeriğinin korunarak bozulmamış olma halidir.

3.3. Kullanılabilirlik

Bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim, kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesine göre, her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

4. UYGULAMALARA İLİŞKİN KURALLAR

Oda çalışanları, hangi türde olursa olsun elektronik uygulama ve hizmetleri kullanırken üretecekleri ve paylaşacakları içerik bakımından şu kurallara uygun hareket ederler:

4.1. Elektronik Posta Kullanma Kuralları

1. **Oda** elektronik posta sistemi, kullanıcının şahsi sosyal medya (facebook, twitter, instagram vb.) hesapları için kesinlikle kullanılamaz.
2. Kötü amaçlı, spam, sahte vs. nitelikteki zararlı e-postalara yanıt yazılmamalı, bu maillere iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
3. E-posta listeleri ve benzeri bildirim araçlarına kişisel kullanım amacıyla üye olmak için kurumsal e-posta adresleri kullanılamaz.

4. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, bu tür e-postalar herhangi bir işlem yapılmaksızın derhal silinmelidir.
5. Çalışanlar, e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.
6. Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
7. Çalışanlar, kurumsal e-postaların firma dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.
8. Çalışanlar başta kişisel veri ve gizli bilgi içerebilecek olanlar olmak üzere iş amaçlı e-postaların yanlış adreslere gönderilmemesi için daha fazla dikkatli olmalı ve özen göstermelidir.
9. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.
10. Çalışanlar **Oda** tarafından tahsis edilen e-posta metinlerinde standart imza altı uyarı metnini ve kişisel veriler için hazırlanan Ön Aydınlatma Metnini kullanmalıdırlar.
11. Çalışanlar kendilerine ait e-posta adresinin şifresinin güvenliğinden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren bilgi işlem departmanı ile temasa geçip onlara durumu haber vermekle yükümlüdürler.
12. Ayrılan çalışanları, kurumsal e-posta sistemini kullanmaya devam edemez. E-posta adresine sahip kullanıcının birim değiştirme, işten ayrılma gibi herhangi bir sebeple ayırılması durumunda e-posta sisteminde gerekli değişiklikler yetkililer tarafından Bilgi İşlem Birimine en kısa zamanda bildirilir.

4.2. Anlık Mesajlaşma Uygulamaları Kullanma Kuralları

Anlık mesajlaşma uygulamalarını iş amacıyla kullanırken şu kurallara dikkat edilmelidir:

1. Çalışan, müşteri veya diğer ilgililerle yapılacak anlık mesajlaşmalarda ilk olarak ilgili ön aydınlatma metni paylaşılacaktır.
2. Çalışan, müşteri veya diğer ilgililerle yapılacak anlık mesajlaşmalar için ilgili birim yöneticisinin bilgisi dahilinde grup kurulabilecektir.
3. İş amacıyla anlık mesajlaşma uygulamaları üzerinde çalışanlar tarafından oluşturulan grupların açılışında ilk mesajla olarak ön aydınlatma metni paylaşılacaktır.
4. **Oda** tarafından işlenen kişisel verilerin paylaşılması muhtemel iş ve profesyonel amaçla kurulmuş olan üçüncü kişilerin oluşturduğu gruplara üye olunurken, ilgili grubun veri güvenliği ve veri korumaya ilişkin belgelerinin bulunup bulunmadığı kontrol edilecektir.
5. Üçüncü kişiler tarafından oluşturulan grupların veri güvenliği ve veri koruma belgelerinin bulunmaması halinde grup yöneticileri bu sorunla ilgili uyarılacaktır. Gerekli düzeltmelerin yapılmaması durumunda böyle bir grupta hiçbir şekilde kişisel veri içeren mesaj ve belgeler paylaşılmayacak, riskin büyük olduğu düşünülüyor ise çalışan gruptan ayrılacaktır.

4.3. Video Konferans Uygulamaları Kullanma Kuralları

Video konferans uygulamalarını kullanırken şu kurallara dikkat edilecektir:

1. İş amacıyla yapılacak görüşmelerde varsa ve uygunsa **Oda** video konferans uygulama hesaplarının kullanılması tercih edilecektir.
2. Çalışanlarımız tarafından başlatılacak video konferans ve toplantıların sms, anlık mesaj veya e-posta gibi araçlarla yapılacak davetlere ilgili ön aydınlatma metinleri eklenecektir.
3. **Oda** video konferans hesapları hiç bir şekilde kişisel ve özel amaçlarla kullanılmayacaktır.
4. Video konferanslar gerekmedikçe kayıt altına alınmayacak. Kayıt altına alınması gereken durumlarda ise kayıttan önce tüm katılımcıların bilgilendirilecek ve izinleri alınacaktır. Kayıt başladıktan sonra kayıt için katılımcılardan izin alındığı sözlü olarak beyan edilip, onay vermek istemeyenlerin itirazlarını sözlü olarak belirtmeleri istenilecektir.
5. Video konferanslar sırasında iş amacı gerektirmediği sürece üçüncü kişilerin kişisel verileri sözlü veya belge olarak paylaşılmayacaktır.
6. Çalışanlar, kendi hesapları ile katıldıkları iş amaçlı toplantılarda da bu kurallara uyacaklardır.
7. Anlık mesajlaşma uygulamaları ve bunların bünyelerinde oluşturulan **Oda** içi veya dışı grupları kullanırken:

4.4. Sosyal Medya Hesapları Kullanma Kuralları

1. **Oda** sosyal medya hesapları sorumlu ve görevli birim ve/veya çalışan/çalışanlar tarafından yönetilir.
2. Görevli olmayan kişiler **Oda** sosyal medya hesaplarını kullanamazlar.
3. Görevli olmayan kişilerle sosyal medya hesaplarının bilgileri, kullanıcı adı ve şifreleri paylaşılamaz.
4. **Oda** sosyal medya hesapları bilgi işlemden sorumlu birim de bilgilendirilerek yönetimin izni ve bilgisi dahilinde açılır veya kapatılır.
5. Sosyal medya hesapları üzerinden paylaşımlar görevli birim amirinin bilgisi dahilinde ve görevli çalışan tarafından yapılır. Görevlendirilenler dışında hiç kimse sosyal medya hesapları üzerinden paylaşımda bulunamaz.
6. Sosyal medya hesaplarında temel belgeler ve ilgili alanlara, takipçilerin kolayca görebileceği şekilde ilgili aydınlatma belgeleri yerleştirilecektir.
7. Sosyal medya hesaplarının takipçilerine ait veriler görevli birim ve sorumlu dışında ve yönetim haricinde **Oda** içinde ve dışında paylaşılmayacaktır.
8. Sosyal medya hesaplarında paylaşılacak çalışan, müşteri ve diğer taraflara ait görseller ve videolar için ilgililerin açık rızasının alınmasına dikkat edilecektir.
9. Sosyal medya uygulamaları kullanılırken:

4.5. İnternet Kullanma Kuralları

1. Hiçbir kullanıcı **Oda** tarafından tavsiye edilen veri paylaşım yöntemi dışındaki bir veri paylaşım kanalını kullanamaz. (Örneğin; Bittorent, iMesh, eDonkey, Aimster vb. peer-to-peer bağlantı yollarını içeren programlar kullanılamaz.)
2. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde mesajlaşma ve sohbet programları gibi chat programları kullanılarak kişisel veri toplanamaz.
3. Hiçbir kullanıcı özel amaçlı olarak internet üzerinden Multimedia Streaming (Video, müzik ve iletişim vb. için) yapamayacaktır.
4. İş ile ilgili olmayan (Müzik, video dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek (download) etmek ve bilgisayarlarda saklamak yasaktır.
5. İnternet üzerinden Bilgi İşlem Birimi tarafından onaylanmamış yazılımlar indirilemez ve firma sistemleri üzerine bu yazılımlar kurulamaz, kullanılamaz.
6. **Oda** ağlarından ve bilgisayarlarından genel ahlak anlayışına aykırı internet Site ine girilmemeli ve dosya indirimi yapılmamalıdır.
7. Bilgi İşlem Birimi, iş kaybının önlenmesi için çalışanların internet kullanımı hakkında gözlemleme ve istatistik yapabilir. Gerekli durumlarda internet üzerinde kısıtlamalar yapabilir.
8. Herhangi bir siyasi içerik ya da propaganda yapılamaz.

4.6 İnternet Erişimi Sağlama Kuralları

1. Kullanıcılar **Oda** tarafından sağlanan ağ yapısı üzerinden konusu suç teşkil edebilecek, genel ahlak anlayışına aykırı veya kişileri zarara uğratabilecek site ve uygulamalara erişim sağlayamazlar,
2. **Oda** tarafından internete sağlanan erişime ilişkin log kayıtları modem veya uygun araç ve sistemler üzerinde tutulur
3. **Oda** ağlarını kullanarak internete erişim sağlayan ziyaretçilerden kişisel verilerinin işlenmesi için açık rızaları alınır
4. **Oda** tarafından sağlanan internet erişimini gerekli gördüğü durumlarda genel ve bireysel olarak kısıtlayabilir veya durdurabilir

5. GENEL KURALLAR

5.1. Genel Kullanım Kuralları

1. Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve üçüncü şahısların bilgilere erişimi engellenmelidir.

2. Taşınabilir bilgisayarların ekranları mutlaka şifreli ekran koruyu ile kilitlenmelidir.
3. **Oda** verilerini içeren bir bilgisayarın, tabletin veya mobil cihazın çalınması, kaybolması vs. durumlar en kısa sürede Bilgi İşleme bildirilmelidir.
4. Bütün kullanıcılar kendi cihazlarının sistem güvenliğinden sorumludur. Bu cihazlardan kaynaklanabilecek **Oda** veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret veya siyasi içerikli mail, kullanıcı bilgileri vs.) kişi sorumludur.
5. **Oda** bilgisayarlarını kullanarak taciz, hakaret vb. yasadışı olaylara karışılmamalıdır.
6. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak (packetsniffing, packetspoofing, denial of service vb.) eylemlere girişilmemelidir.
7. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.
8. **Oda** bilgileri üçüncü kişilere iletilmemelidir.
9. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
10. Herhangi bir cihaz, yazılım ve veri izinsiz olarak **Oda** dışına çıkarılmamalıdır.
11. **Oda** tarafından kullanılan yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD'leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.
12. Personel, kendilerine tahsis edilen ve **Oda** çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliğinden sorumludur.
13. Bilgi İşlem Birimi kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir, gereken teknik veya idari tedbirleri uygulayabilir.
14. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
15. Bilgisayarlar üzerinde resmî belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
16. **Oda** Bilgi İşleminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-Posta Servisi vb.) sunucu niteliğinde olan bilgisayar ve cihaz bulundurulmamalıdır.
17. Bilgi İşlemin bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.
18. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisanssız yazılımı bilgisayarında barındıran personel bu durumdan kendisi sorumludur.
19. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde mutlaka şifre kullanım kurallarına göre hareket edilmelidir.
20. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşleme haber verilmelidir.

5.2. Acil Durum Kuralları

1. **Oda** 5651 sayılı yasa gereğince log kayıtlarını imkanları nispetinde tutmaya özen gösterir.
2. Acil durumlar için sistem logları incelenmek üzere saklanmalıdır.
3. **Oda** faaliyetlerinin devamlılığını sağlamak esastır.
4. Veri Güvenliği olayları ve veri ihlalleri ilgili Politika Belgesi ve Yönergede belirtilen usul ve esaslara göre yönetilir.
5. Acil durumlar için gerekli araç-gereç ihtiyaçları tespit edilerek, yedekleme ve bakım planlaması yapılarak uygulanmalıdır.

5.3. Antivirüs Kuralları

1. Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem Birimine haber verilmelidir.
2. Zararlı programları (Örneğin, virüsler, solucanlar, truva atı, e-posta bombaları vb.) **Oda** bünyesinde oluşturmak ve dağıtmak yasaktır.

3. Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını kuramaz.

5.4. Şifre Kullanma

Şifreleme, bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre, ağ güvenliğini tümüyle riske atabilir. Güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkındaki standartlar ve uyulması gereken kurallar aşağıda belirtilmiştir.

5.4.1. Şifre Kullanma Kuralları

1. Kullanılan şifrelerin tamamı kolayca kırılamayacak güce sahip olmalıdır.
2. Şifreler (E-posta, internet, PC vs.) en az altı ayda bir değiştirilmelidir.
3. Şifreler e-posta iletilerine veya herhangi bir elektronik forma yazılmamalı ve eklenmemeli, başkası ile paylaşılmamalı, fiziki ya da elektronik ortamlara yazılmamalıdır.
4. Herhangi bir kişiye telefonda şifre verilmemelidir.
5. Şifreler, işten uzakta olunan zamanlarda dahi iş arkadaşlarıyla paylaşılmamalıdır.
6. Kullanıcı, şifresini 3. kişilerle paylaşmamalı, kağıtlara ya da elektronik ortamlara yazmamalıdır.
7. Şifre 5 defa üst üste yanlış girildiğinde bilgisayar kilitlenmektedir.
8. Çoklu giriş yapılan bilgisayarlara giren personellere uyarılar yapılmaktadır.
9. Mutlaka ekran kilidi kullanılmalı ve ekran kilidi kısa aralıklara ayarlanmalıdır.

5.4.2. Genel Şifre Oluşturma Kuralları

1. Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs.). Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.
2. Şifre, küçük ve büyük karakterlerle (a-z, A-Z), rakam ve sembollere (0-9, !'^+%&/()=?_;* gibi) sahip olmalıdır.
3. En az sekiz karakter olmalıdır.
4. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıdan şifresini değiştirmesi talep edilecektir.

5.4.3. Şifre Koruma Kuralları

1. **Oda** bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmamalıdır. (Örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde).
2. Değişik sistemler için farklı şifreleme kullanılmalıdır. Örneğin, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanılmalıdır.

5.4.4. Şifrelerle ilgili şunlar yapılamaz

1. Herhangi bir kişiye telefonda şifre vermek.
2. E-posta mesajlarında şifre belirtmek.
3. Üst yöneticinizle şifreleri paylaşmak.
4. Başkaları önünde şifreler hakkında konuşmak.
5. Aile isimlerini şifre olarak kullanmak.
6. Herhangi bir form üzerinde şifre belirtmek.
7. Şifreleri aile bireyleri ile paylaşmak.
8. Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmek.
9. Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini araması söylenmelidir.
10. Uygulamalarda ve browserlardaki "şifre hatırlama" özellikleri seçilmemelidir. (Örnek: Chrome, Internet Explorer vs.)

5.5. Uygulama Geliştirme Kuralları

1. Uygulama geliştiricileri programlarında aşağıda belirtilen güvenlik özelliklerinin sağlandığından emin olmalıdırlar.
2. Bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.
3. Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.
4. Kural yönetim sistemi desteklenmelidir. (Örnek; bir kullanıcı diğer bir kimsenin şifresini bilmeden fonksiyonlarına devam edebilmelidir.)

5.6. Uzaktan Erişen Kullanıcılar için Şifre Kullanımı

Oda bilgisayar ağına uzaktan erişimi tek yönlü şifreleme algoritması veya güçlü şifrelerle yapılmalıdır.

5.7. Sunucu Güvenliği

Sunucuların güvenliğinin sağlanması için uyulması gereken kurallar ve standartlar şunlardır.

5.7.1. Sahip Olma ve Sorumluluklar

1. **Oda** bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur.
2. Sunucu konfigürasyonları sadece bu grup tarafından yapılacaktır.
3. Bütün sunucular ve mobil cihazlar ilgili **Oda** cihaz envanterinde kayıtlı olmalıdır. Envanter en az aşağıdaki bilgileri içermelidir:
4. Kişisel veri güvenliğine ilişkin tedbirler alınmak kaydıyla **Oda** bütün bilgilerin güncel olarak tutulmalıdır.
5. **Oda** tarafından izin verilen bilgi işlem sistemleri haricinde yabancı bir mobil cihaz ya da veri taşıyıcı takılamaz, kullanılamaz.

5.8. Genel Konfigürasyon Kuralları

1. İşletim sistemi konfigürasyonları bilgi işlem biriminin talimatlarına göre yapılacaktır.
2. Kullanılmayan servisler ve uygulamalar kapatılacaktır.
3. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
4. Uygulama erişimleri için standart güvenlik prensiplerini çalıştırılmamalı, gereksiz servisler açılmamalıdır.
5. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
6. Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
7. Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.

5.9. Gözlemleme

1. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır:
2. Bütün güvenlikle ilgili loğlar minimum 1 hafta saklanmalıdır ve online olarak erişilmelidir.
3. Günlük tape backupları en az 1 ay saklanmalıdır.
4. Logların haftalık tape backup'ı en az 1 ay tutulmalıdır.
5. Aylık full backuplar en az 6 ay tutulmalıdır.
6. Logloma kayıtları bina dışında olmalıdır.
7. Güvenlikle ilgili loğlar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikli ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.
8. Port tarama atakları.

9. Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.
10. Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

5.10. Uygunluk

1. Denetimler yetkili organizasyonlar tarafından **Oda** bünyesinde atanan **Komite** tarafından altı ayda bir yapılacaktır.

2. Denetimler Bilgi İşlem Birimi tarafından yönetilecektir.

3. Denetimlerde organizasyonun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

5.11. İşletim

1. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

2. Sunucuların yazılım ve donanım bakımları yılda bir yetkili uzmanlar tarafından yapılmalıdır.

3. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

5.12. Kimlik Doğrulama ve Yetkilendirme

1. Bilgi sistemlerinde Kimlik Doğrulama ve Yetkilendirme, konusunda alınması gereken önlemler, uyulması gereken kurallar ve standartlar şunlardır:
2. **Oda** sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.
3. **Oda** sistemlerine erişmesi gereken kurum dışı ve extranet kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacaktır.
4. **Oda** bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenmelidir.
5. Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
6. Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir.
7. Kullanıcılar **Oda** adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.
8. Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
9. Sistemlere log-in olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.
10. Kullanıcılara erişim hakları yazılı olarak beyan edilmeli ve erişim haklarını ihlal eden kullanıcılar için yaptırım uygulanmalıdır.
11. Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
12. Dışarıdan **Oda** wi-fi ağına bağlanacak kimselerin mutlaka kimlik tespiti yapılmalıdır. Toplantı odaları için tahsis edilen wi-fi şifre kullanımları da toplantıya katılanların kimliği ile eşleştirilmelidir.

5.13. Denetim ve Kontrol

Oda, çalışanlara tahsis ettiği cihazlar, e-posta ve uygulama hesapları üzerinde kurumsal yapısını ve servislerini zarara uğratan veya uğratacağından şüphelenilen, hukuka aykırı kullanım şüphesi veya performans ve kalite amaçlı denetim ve kontroller yapabilir.

5.14. Kişisel Veri Aktarımında Gözetilecek Hususlar

1. Kişisel veri paylaşımı sırasında veri aktarılan tüm taraflar ile bir veri aktarım sözleşmesi, taahhütname veya benzeri belgelerin imzalanması yoluyla veri aktarımının güvence altına alınması sağlanır.
2. Her bir birim ve çalışan kişisel veri aktarımı yapılan muhatabın kişisel verilerle ilgili oluşturabileceği riskleri önceden gözetmeli ve risk yaratacak durumların oluşmaması için özen göstermelidir.
3. Yurt dışı menşeli uygulama ve servislerin kullanımında Kanun ve gibi ilgili mevzuata uyum konusunda özen gösterilir.

4. Taraflar ve tedarikçilere yapılacak veri aktarımları esnasında veri güvenliğinin uygun ve güvenli araç ve kanallarla yapılması, kişisel verilerin aktarıldığı gerçek kişilerin muhatap tarafından yetkilendirilmiş olup olmadığının takip edilmesi, kişisel verilerin aktarım amacıyla oluşturulan nüsha ve kopyaları varsa bunların işlevleri sona erer ermez tüm mecralardan silinmesine dikkat edilmesi zorunludur.
5. **Oda** birim ve çalışanları veri aktardıkları taraf ve tedarikçilerin kişisel veriler konusundaki hassasiyetlerini ve uygulamalarını gözetmek, risk oluşturabilecek durumları üstlerine zamanında bildirmekle yükümlüdürler. **Oda** çalışanları kişisel veriler konusunda çözümleyemedikleri durum ve sorunlar konusunda zamanında üstlerinden gerekli desteği istemelidirler.

6. KİŞİSEL VERİLERİN GÜVENLİĞİ

6.1. Genel Kurallar

Oda tarafından işlenen kişisel ve kurumsal bilgilerin güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

1. **Oda** bünyesinde kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin nitelikli verilere erişmesi mümkün olmamalıdır.
2. Kişisel veriler, kişiye aittir. Yetkilendirilmiş çalışanlar ancak görevleri ile ilgili kişisel verilere erişebilmelidirler. Ancak **Oda** bünyesinde atanmış bulunan ilgili sorumlunun yazılı onayı ile diğer yetki dışındaki kişiler verilere erişebilirler.
3. Veri sahibi kişinin rızası olmadan hiçbir çalışan sözle de olsa ilgili kişinin bilgilerini kişinin yakınları ile ya da tanıdıkları gibi üçüncü şahıslara ve kurumlara iletemez.
4. Veri sahibi kişinin anlaşmalı hekim vb. kişilerin verileri ticari amaçlı olarak da üçüncü şahıslara iletilemez.
5. Veri sahibi kişinin talebi halinde bilgilerine ilişkin bir kopya kendilerine teslim edilmelidir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir kayıt, elektronik veya kâğıt ortamında üçüncü kişi ve kurumlara verilmemelidir.
6. Veri sahibi kişiye ait kişisel verilerin izlenmemesi için gerekli tedbirler alınmalıdır. (Kişisel veri içeren hiçbir kayıt gelişi güzel ortada bırakılmamalı, bilgisayar ekranı başkalarınca okunabilecek şekilde bırakılmamalıdır).
7. Telefon ile konuşurken kişisel verilere üçüncü şahısların duymasına engel olunmalıdır.
8. Bütün kişisel veriler fiziksel olarak korunmuş mekanlarda saklanmalıdır. Evrakın **Oda** içinde ya da Avukat, YMM ya da YGM gibi paydaşlarla fiziksel olarak paylaşılması söz konusuysa, evrak kapalı ve KİŞİSEL VERİ İÇERİR uyarılı zarflar içerisinde taşınmalıdır.
9. **Oda** elektronik kayıtlarına internet ortamından yetkisiz erişim mümkün olmamalıdır.

6.2. Özel Nitelikli Kişisel Verilerin Güvenliğine İlişkin Kurallar

Oda tarafından işlenen ve tutulan özel nitelikli veriler ilgili politika belgesine uygun olarak işlenir.

7. GÜNCELLEME

İş bu politika belgesi, **Oda** kişisel veri işleme şartları, araçları, amaçları ile kapsamı değiştiğinde ve kişisel verilerin paylaşıldığı tarafların değişmesi durumlarında güncellenir.

8. İLGİLİ ARAÇLAR VE KAYNAKLAR

8.1 İlgili Kontrol ve Güvence Araçları

1. Gizlilik Politikası
2. Veri Güvenliği Olay Yönetimi ve Veri İhlal Bildirimleri Politikası
3. Kişisel Veri Saklama, Silme, İmha ve Aktarma Politikası
4. Çerez Politikası
5. Veri Güvenliği Olay Yönetimi ve Veri İhlal Bildirimleri Yönergesi
6. Kişisel Veri Envanteri
7. Veri İşleme Sözleşmeleri

8.2 Dış Kaynaklar

1. 6698 sayılı Kişisel Verilerin Korunması Kanunu
2. KVKK Kişisel Veri İhlal Bildirim Formu Klavuzu
3. KVKK Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)
4. Biyometrik Verilerin İşlenmesinde Dikkat Edilmesi Gereken Hususlara İlişkin Rehber
5. Yapay Zeka Alanında Kişisel Verilerin Korunmasına Dair Tavsiyeler

Daha fazla bilgi için **Komite** ile temas kurabilirsiniz.