1. AMAÇ

Bilgi Güvenliği ve Kalite Yönetim Sistemi'nin ALOTECH İLETİŞİM TEKNOLOJİLERİ TİCARET A.Ş 'nin içerisinde sürdürülebilirliğin sağlanabilmesi için Bilgi Güvenliği Yönetim Sistemi Ekibi başta olmak üzere ilgili çalışan ve üçüncü taraf kişi/kurumların yapması gereken çalışmaların temel kurallarını belirlemeyi amaçlamaktır.

2. KAPSAM

Bu politika ALOTECH İLETİŞİM TEKNOLOJİLERİ TİCARET A.Ş 'nin bilgi varlıklarının gizliliği, bütünlüğü ve kullanılabilirliğini etkileyen tüm unsurları ve çalışma ortamlarını kapsamaktadır.

3. SORUMLULUK

Uygulama politikasının, gözden geçirilmesi ve güncellenmesinden BGYS Yönetim temsilcisi ve BGYS Ekip Üyeleri sorumludur. Bu politikalara uyulmasından iç ve dış personeller sorumludur.

4. TANIMLAR

BGYS: Bilgi güvenliği Yönetim Sistemi

5. POLİTİKA

5.1. Bulut Kullanım Kuralları

a) Bulut hizmetlerini kullanmadan önce, çalışanlarımızın bilgi güvenliği politikalarını ve prosedürlerini anlamaları ve uygulamaları gerekmektedir.
b) Hassas veya gizli bilgileri bulut hizmetlerine yüklerken, şifreleme kullanarak veriler korunmalıdır.
c) Bulut hizmetlerindeki kullanıcı kimliklerini ve erişim yetkilerini düzenli olarak gözden geçirerek, yetkisiz erişimler önlenmelidir.
d) Bulut hizmetlerine erişimde çok faktörlü kimlik doğrulama (örneğin, şifre ve SMS doğrulama kodu) kullanılmalı.
e) Bulut hizmetlerinde güçlü şifreleme algoritmaları ve güvenli iletişim protokolleri kullanılmalıdır.
f) Bulut hizmetlerinde kaydedilen logları ve izleme verilerini düzenli olarak incelemeli ve anormal aktiviteleri tespit edilmeli.

5.2. Veri Maskeleme Kuralları

a) Kişisel verilerin gizliliğine özen göstermeli ve veri maskeleme yöntemlerine uygun şekilde kullanmalıdır.
b) Maskeleme işlemi sonucunda elde edilen verilerin gizliliğini korumalı ve yetkisiz erişimlerden kaçınmalı.
c) Maskeleme sürecini doğru bir şekilde uygulamalı ve veri maskeleme yöntemlerini gerektiği gibi anlamalı.

d) Maskeleme sonrası verileri dikkatlice kullanmalı ve sadece ihtiyaç duyduğunuz alanlarda erişim sağlamalı.
e) Maskeleme işlemi sırasında kullanılan araçları ve yazılımları lisanslı ve güncel tutmalı.
f) Maskeleme sonrası verilerin korunması için gerekli güvenlik kontrollerini uygulamalı.
g) Maskeleme süreciyle ilgili politikalara ve kurum içi yönergelerine tam uyum sağlamalı.
h) Maskeleme yapılan verilerin tamamen silinmesi gerektiğinde, gereken adımları atarak verileri güvenli bir şekilde yok etmeli.
i) Veri maskeleme yöntemlerini kullanırken, kurumun ve müşterilerin güvenliğini en üst düzeyde tutmaya özen göstermeli.
j) Maskeleme işlemiyle ilgili herhangi bir sorun veya güvenlik açığı tespit ettiğinizde hızla ilgili birime bildirim yapmalı ve gereken önlemleri almalı.

5.3. Antivirüs Programı Uygulama Kuralları

a) Kurumun bütün bilgisayarları ve sunucuları anti-virüs yazılımına sahip olmalıdır.

b) Düzenli aralıklarla anti-virüs yazılımı otomatik veya manuel olarak güncellenecektir.

c) Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmamalıdır.

d) Hiçbir kullanıcının herhangi bir sebepten dolayı anti-virüs programını sistemden kaldırması veya durdurmasını engelleyecek kısıtlamalar yapılmalıdır.

e) Bilinmeyen ve şüpheli bir kaynaktan gelen e-postalar Bilgi İşlem Birimi tarafından kontrol edilmelidir. Yapılan kontroller kurum ağından izole edilmiş bir ortamda yapılmalıdır.

f) Taşınabilir bilgi depolama cihazları resmi ve onaylı kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.

g) Taşınabilir depolama aygıtının Şirket dışı bir bilgisayara takılması gereken durumlarda, anti-virüs programının bulunduğundan ve güncel olduğundan emin olunmalıdır. Anti-virüs programı olmayan bilgisayara taşınabilir depolama aygıtları takılmamalıdır.

h) Kurum ağına anti-virüs programı güncel olmayan bilgisayarlar dâhil edilmemelidir.

5.4. Sunucu Güvenlik Kuralları

a) Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.

b) Bütün sunucular (kurumun sahip olduğu) ilgili envanter listesine kayıtlı olmalıdır.

c) Sunucu işletim sistemleri üzerindeki kullanılmayan servisler ve uygulamalar kapatılmalıdır. Port açma talepleri yazılı olarak alınmalı ve alınan talepte portun açık kalma süresi beyan edilmelidir.

d) Kullanılmayan sunucular güvenlik ve elektrik tasarrufu açısından kapalı tutulmalıdır.

e) Sunucular üzerinde yapılan işlemlerin log kayıtları en az 1 hafta saklanacak şekilde ayarlanmalıdır.

f) İşletim sistemleri, uygulamalar, veri tabanları, ağ donanımları yetkili erişim logları tutulmalıdır.

g) Sunucuların yönetimi için her sunucunun kendi hesabı ile bağlantı yapılmalıdır. Sunuculara dışarıdan yapılan bağlantılar uzak bağlantıya ilişkin belirlenen kurallara göre yapılmalıdır.

h) Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulunmalıdırlar.

i) Sistem odaları sıcaklık değerleri ve su basmasına karşı denetlenmelidir.

j) Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt altına alınmalıdır. Sistem odası sunucu bakımları refakatçi kontrolünde olmalıdır.

k) Elektrik ve data kabloları sunucu odaları dahil kurum içerisinde kanallardan geçmelidir.

l) Sistem odalarındaki ekipmanların bakımları düzenli olarak yapılmalı ve bakımlar kayıt altına alınmalıdır.

5.5. Ağ Yönetim Kuralları

a) Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedekli ekipman bulundurulmalı veya bakım anlaşmaları yapılmalıdır.
b) Ağ ekipmanları sadece yetkilendirilmiş kişiler tarafından erişilebilir ve yönetilebilir olmalıdır. Yetkisiz erişime karşı korunmalıdır.
c) Kurum ağına sadece kurum bilgisayarları bağlanmalıdır. Kurum dışında bir bilgisayar bağlanacak ise yetkili kişinin izni ve gözetiminde bağlanmalıdır.
d) Kurum internet ağına misafirler alınmamalı, misafir ağı kurum ağından bağımsız tasarlanmalıdır.
e) Kamera, santral, kablosuz ağ, kullanıcı ağları vb. ağlar birbirinden ayrı olmalıdır.
f) Uzaktan bağlantı, kamera vb. için kabul görmüş varsayılan portlar kullanılmamalı ve portların güvenliği sağlanmalıdır.
g) Ağ cihazları yılda en az 1 defa açıklık tarama testlerinden geçirilerek güvenli hale getirilmelidir.
h) Ağ cihazlarının konfigürasyonları kritik değişikliklerden sonra veya belirli periyotlarda yedeği alınarak saklanmalıdır.
i) Harici web sitelerine erişim, kötü amaçlı içeriğe maruz kalmayı azaltacak şekilde yönetilmelidir.

5.6. Uzak Bağlantı VPN Kuralları

a) Uzaktan bağlantılar sadece güvenli uygulamalar ile yapılmalıdır.

b) Üçüncü taraflar kendi sunucularına, tanımlanmış IP adresleri üzerinden RDP ile bağlantı kuracak şekilde ayarlanmalıdır.

c) Kurum ağ sistemleri ve donanımlarına sadece kurumun onay verdiği ofis ortamında bulunan yerel donanımların bağlanmasına izin verilir. Bunun dışında kurum dışından sağlanan bağlantılar için güvenli ağ erişim protokolleri (SSL VPN, SSH vb.) uygulanarak uzaktan erişim sağlanır. Uzaktan erişimlerde 2FA ve üzeri güvenlik önlemleri uygulanmalıdır.

d) VPN kullanım hakkı verilen kişiler firewall üzerinde listelenmeli ve düzenli olarak kontrol edilmelidir.

e) Uzak bağlantı yapan kurum dışı bilgisayarlar, Anti-virüs Politikasına uygun bir şekilde cihazların anti-virüs yazılımları kurulu ve güncel olmalıdır.

f) Sadece kurumun onay verdiği kullanıcılar VPN 'i kullanabilir.

g) Kurum personeli dışında üçüncü taraflara verilecek erişimler için gizlilik anlaşması yapılmış olmalıdır.

h) Uzak bağlantı yetkileri sadece gizlilik taahhüdü alınmış üçüncü taraf kişi/kurumlara verilmelidir.

i) Şirket ağına uzaktan erişim sağlayacak olan üçüncü taraflara ait bilgisayarların, işletim sistemi ve antivirüs yazılımı güncellemelerinin yapılmış olmasından bağlantı sahibi olan kişi sorumludur. Sorumluluk sözleşme ile verilmelidir.

j) Tanımlanmış VPN hesabı ile aynı zaman içerisinde birden fazla bağlantı yapılmamaktadır.

k) Uzak bağlantı yetkileri sadece gizlilik taahhüdü alınmış üçüncü taraf kişi/kurumlara verilmelidir.

l) Uzaktan erişim bilgileri kullanıcıya Bilgi Teknolojileri tarafından e-posta ile bildirilir

m) Kurum dışı masaüstü bağlantısı ya da VPN üçüncü taraf kişi / kurumlar ile gizlilik ihtiva eden sözleşmeler imzalanır. Gizlilik ihtiva eden, sözleşmesi olmayan üçüncü taraf kişi / kurumlara uzaktan bağlantı yetkisi verilmez.

5.7. Tedarikçi ve Üçüncü Taraf Güvenlik Kuralları

a) Tedarikçiler, bakım firmaları veya üçüncü taraflar (müşteriler) bilgi sistemlerimize veya bilgi varlıklarımıza bakım vb. amaç ile geldiklerinde gizlilik anlaşması yapılması gerekmektedir.

b) Üçüncü taraflar kurum içerisinde bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.

c) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerinde veya bilgi varlıkları üzerinde yapacakları çalışmaları Yönetim Temsilcisine bildirilmelidir.

d) Tedarikçiler, bakım firmaları veya üçüncü taraflar kurumun bilgi sistemlerine kendilerine verilen yetki kapsamında erişim sağlayabilirler.

e) Tedarikçiler, bakım firmaları veya üçüncü taraflara verilen erişim yetkileri, erişim amaçlarına uygun olarak sadece çalışma alanlarında olacak şekilde kısıtlı verilmeli, logları saklı tutulmalı ve çalışma bittikten sonra verilen yetkiler hemen geri alınmalıdır.

f) Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerine ve bilgi varlıklarına eriştikleri süre boyunca refakatçisiz bırakılmamalıdır.

g) Üçüncü taraflara erişim izni verilecek donanımlar (bilgisayar, sunucu vb.) için uzak bağlantı VPN kuralları uygulanacaktır. ALOTECH, bilgi güvenliğine etki edebilecek bir risk görmesi durumunda tedarikçi, bakım firmaları veya üçüncü tarafların erişimlerini herhangi bir uyarıda bulunmadan kesebilir.

h) Tedarikçilerin Kişisel Verilerin Korunması Politikası kurallarına uygun hareket etmesi istenmelidir.

i) Kişisel verilerin kullanılmasını gerektiren sebeplerin ortadan kalkması hâlinde verilerin aktarıldığı 3.taraf kişi/kurumlar bilgilendirilmelidir.

5.8. Mobil ve Taşınabilir Cihaz Yönetim Kuralları

a) Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.

b) Etki alanındaki bilgisayarların admin yetkileri sınırlandırılarak yalnızca user yetkilendirmesi ile ilgili kişiye teslim edilmelidir.

c) Taşınabilir cihazlar (tablet, laptop) teslim edilmeden önce şifre belirlenmelidir. Şifreler sadece kullanıcının kendisine teslim edilmelidir. Kullanıcı ilk oturum açmasında şifre değiştirmeye zorlanacak şekilde kural oluşturulmalıdır.

d) Etki alanı dâhilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar ilgili kişiye yetki verilmiş ortak alana kaydedilmelidir.

e) Taşınabilir cihazlara kurum dışında meydana gelecek bilgi güvenliği zafiyetlerine karşı (hırsızlık, bakım ve onarım faaliyetleri vb.) şifreleme güvenliği (encrypt) kullanılmalıdır.

f) Kullanıcılar, uç nokta cihazlarında yalnızca güvenilir uygulamaları yüklemeli ve kullanmalıdır.

5.9. Veritabanı Güvenlik Kuralları

a) Veri tabanında bulunan kişisel ve kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir. Log kayıtlarına yetkisiz erişimlere karşı kısıtlama yapılmalıdır.
b) Veri tabanı sunucusuna sadece yetki hakkına sahip olanlar bağlanmalıdır.
c) Hassas verilerin işlendiği, depolandığı veya iletilen sistemler, ağlar ve diğer cihazlar, veri sızıntısı önleme tedbirlerine tabi tutulmalıdır.
d) Veri sızıntısını önlemek için uygun teknik ve organizasyonel önlemler alınmalıdır.
e) Çalışanlar, veri sızıntısı önleme politikaları ve prosedürleri konusunda eğitilmeli ve bilinçlendirilmelidir.
f) Veri tabanı bulunan sistemlere erişim yetkileri kayıt altına alınmalı ve bu yetkiler kontrol edilmelidir.
g) Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme kuralları oluşturulmalıdır. Yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması sağlanmalıdır.
h) Bilgilerin saklandığı sistemler, fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
i) Veri tabanı sistemlerinde yapılacak bakım onarım, yama ve güncelleme çalışmalarından önce ilgili birimlere duyuru yapılmalıdır.
j) Veri tabanına acil erişim gerekmesi durumunda aksiyon öncesinde ve sonrasında ilgili birimlere veya personellere bilgilendirme yapılmalıdır.
k) Veri tabanı aksiyonlarında destek firmasına talepler yazılı olarak bildirilmelidir.
l) Veri tabanları düzenli olarak yedeklenmelidir.
m) Veri tabanı bulunan medyalar kurum dışına çıkarılmamalıdır.

n) Veri tabanlarının bulunduğu medyaların doluluk oranları düzenli olarak kontrol edilmelidir.
o) Veri tabanı raporları düzenli olarak ilgili firma tarafından verilmelidir.
p) Veri tabanı erişimlerinde üreticinin belirlemiş olduğu default şifreler kullanılmamalıdır.
q) Veri tabanına erişimlerde en az yetki prensibine göre kullanıcının ihtiyacından fazla veriyi görmesi engellenmelidir.
r) Uç nokta cihazlarında veri yedeklemesi düzenli olarak yapılmalıdır.

5.10. Değişim Yönetimi Kuralları

a) Yazılımsal ve donanımsal değişiklik talepleri kayıt altında tutulmalıdır.

b) Değişiklik taleplerinin sözlü olarak alınmaması konusunda hassasiyet gösterilmelidir.

c) Bilgi sistemlerinde değişiklikler yetkilendirilmiş kişiler tarafından yapılmalıdır. Yazılımsal değişikliklerin yetkisiz kişiler tarafından gerçekleştirilmemesi için sistemlerde yetki sınırlaması yapılmalıdır.

d) Herhangi bir sistemde uzun süreli veya önemli değişiklik yapmadan önce bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmelidir.

e) Mevcut sistemlerin kaynaklarının izlenmeli, sorun yaşanmaması adına gerekli önlem ve tedbirler alınmalıdır. Kapasite kullanımının yüksek olması durumlarında kapasite kullanımı düşürülmelidir. (Kullanılmayan servislerin kapatılması, gereksiz dosyaların silinmesi vb.) Kapasite kullanımının düşürülememesi durumunda satın alma faaliyeti gündeme alınmalıdır.

f) Değişiklikler gerçekleştirilmeden önce ilgili birimlere / kişilere bilgi verilmelidir.

g) Yapılacak değişiklikten önce değişikliğin yapılacağı sistemlerin yedekleri alınmalıdır.

h) Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticilere bilgi verilmelidir.

i) Ticari programlarda yapılacak değişiklikler ilgili üretici tarafından onaylanmış kurallar çerçevesinde gerçekleştirilmelidir.

j) Yapılacak değişiklikler mümkün olduğunca test sunucuları üzerinde gerçekleştirilmelidir. Yapılan testlerin başarılı geçmesi halinde canlı sistemde değişiklikler gerçekleştirilmelidir.

k) Değişiklik yapılan donanımların sistem saatlerinin mevcut sistemler ile aynı olmasına dikkat edilmelidir.

l) Yazılımlar için yayınlanmış yamalar önce test edilmeli, sonra ilgili sistemlere yüklenmelidir.

m) Değişikliklere ilişkin kullanıcı ve yönetici log kayıtları alınmalı ve uygun koşullarda saklanmalıdır.

5.11. Kimlik Doğrulama ve Yetkilendirme Kuralları

a) Kullanıcı yetkileri, ilgili kullanıcın yöneticisinin talebiyle verilmeli veya kaldırılmalıdır.

b) Kimlik doğrulama bilgileri ilgili kullanıcının kendisine verilmelidir. İlk verilen kimlik doğrulama bilgileri kolay olmamalı ve ilk oturum açmada sistem tarafından değiştirilmeye zorlanmalıdır.

c) Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenmelidir.

d) Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanmalıdır.

e) Kurum bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli ve kontrol altında tutulmalıdır.

f) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

g) Sistemlerin başarılı ve başarısız erişim logları düzenli olarak tutulmalıdır.

h) Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve kayıt alınmalıdır.

i) Kullanıcı hatalarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

5.12. Olay İhlal Bildirim ve Yönetim Kuralları

a) Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumlarında mutlaka kayıt altına alınmalıdır.

b) Bilgi güvenliği olay raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.

c) Bilgi güvenliği ihlâli oluşması durumunda, kişilerin tüm gerekli faaliyetleri değerlendirmesi Bilgi Güvenliği Yönetim Sistemi ekibi ile birlikte yapılmalıdır.

d) İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.

e) Normal olasılık planlarına ilave olarak olayın tanımı ve sebebinin analizi, önleme, tekrarı önlemek maksadıyla düzeltici tedbirlerin planlanması ve uygulanması, olaylardan etkilenen veya olaylardan kurtulanlarla iletişim, eylemin ilgili otoritelere raporlanması konuları göz önüne alınmalıdır.

f) Adli incelemelerin yürütülebilmesi veya üretici firma kaynaklı zararların telafi edilmesi için ihlalin log kayıtları toplanmalı ve korunmalıdır.

g) Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınmalıdır.

h) Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe, yeni kontrollerin oluşturulması, olayların kök nedenine inilmesi ve yazılı hale getirilmesi gerekmektedir.

i) Kanıt toplama faaliyetinde aşağıdaki süreçler takip edilmelidir;

- Kanıtın niteliği ve tamlığını gösteren içerik.
- İhlale neden olan olayların kanıtları için kamera kayıtları, giriş çıkış kayıtları, sunucu/program ve bilgisayar logları, firewall logları ve internet logları.
- Olay kanıtlarının korunması yetkili kişilerin dışında erişimi kapatarak veya yedekleme yaparak sağlanır.

k) Kişisel veriler ile ilgili bir ihlal gerçekleşmesi durumunda aynı gün Veri Sorumlusu İrtibat Kişisi bilgilendirilmelidir. İhlal Veri Sorumlusu İrtibat Kişisi tarafından 3 gün içerisinde KVKK 'ya https://ihlalbildirim.kvkk.gov.tr adresinden bildirilmelidir.
l) Tehdit istihbaratı, düzenli olarak güvenilir kaynaklardan toplanmalı ve analiz edilmelidir.
m) Tehditlerin potansiyel etkileri ve riskleri değerlendirilmeli ve buna göre önceliklendirme yapılmalıdır.
n) İç ve dış kaynaklardan alınan tehdit istihbaratı, doğruluk ve güvenilirlik açısından değerlendirilmelidir.
o) Tehdit istihbaratı süreçleri, uygun şekilde belgelenmeli ve düzenli olarak gözden geçirilmelidir.

5.13. Erişim Kontrolleri

a) Kurum içerisinde giriş çıkışlar kamera sistemi ile kayıt altına alınmalıdır.

b) Aktif dizine bağlanan kullanıcı parolaları Parola Yönetim Kurallarına uygun tanımlanmalıdır.

c) Ağ üzerinde aktif dizin kullanıcıları için ortak alanlar oluşturulmalıdır. Bu ortak alanlar üzerindeki birimler ve kullanıcılara göre yetkilendirme yapılmalıdır.

d) Yetkilendirilen personel haricinde hiçbir personelin dosya silme yetkisi bulunmamalıdır.

e) Kurumda mümkün olduğunca SSL ya da benzeri güvenlik protokolleri kullanılmalıdır.

f) Erişim kontrolleri Erişim ve Kullanım Yetki Tablosunda belirtilen kontrol sorumluları tarafından tanımlanmış zaman dilimlerinde gözden geçirilmelidir.

g) Kullanıcılara erişim yetkilerinin verilmesi, hesap tanımlanması, yetkilerin düzenlenmesi veya yetkilerin kaldırılmasına ilişkin talepler ilgili personelin yöneticisi tarafından yazılı olarak alınmalıdır.

h) Ayrıcalıklı erişim yetkileri mümkün olduğunca süre sınırlı olmalıdır.

i) Programların kaynak kodlarına erişim kısıtlanmalıdır.

5.14. Parola Yönetim Kuralları

a) Kullanıcı uç nokta cihazları, güvenli bir parola ile korunmalıdır.

b) Kullanıcı bilgisayar şifreleri 6 ayda bir değiştirilmelidir.

c) Oluşturulacak şifre son 3 parola ile aynı olmayacak şekilde kural belirlenmelidir.

d) Bilgisayar kullanıcı hesaplarının parolaları en az 8 karakter olacak şekilde kural belirlenmelidir. Parola; büyük harf, küçük harf, rakam ve özel karakterden oluşmalıdır.

e) Kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 5 dakika içerisinde şifreli ekran korumasına girecek şekilde kural belirlenmelidir.

f) Kullanıcılara tahsis edilen ilk parola, Parola Yönetim Kurallarına uygun olarak oluşturulmalı ve kullanıcının ilk oturumu açmasıyla yeni parola oluşturmalıdır.

g) ALOTECH çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının parolaları da kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

5.15. Log Yönetim Kuralları

a) Logların yönetimi, log alınacak sistemlerin belirlenmesi ile başlar. ALOTECH 'in kullandığı uygulama, sistem ve erişim log kayıtları alınması KVKK açısından önem arz etmektedir. Yasal ve operasyonel gereksinimler öncelikli olarak göz önünde bulundurulmalıdır. Bu amaçla loglama yapılacağı belirlenen altyapı kaynağında ne tür vakalar için hangi logların üretileceğine ve loglar üzerinde ne tür korelasyon kuralları uygulanacağına Bilgi İşlem Birimi ve varsa anlaşmalı firma ile birlikte karar verilir.

b) Yavaşlama veya sistem kesintisine sebep olmayacak ölçüde log üretilmelidir.

c) Karar verilen log bilgilerinin haricinde, yüksek miktarda loglama yapılmamalıdır.

d) Logların yedekleri kayıtları üreten uygulama, donanım ya da sistem haricinde farklı bir ortama alınması tercih edilmelidir.

e) Log kaynağına ait sistem zamanının tutarsız veya anlamsız olmaması için log kaynaklarına ilişkin saat bilgisi temel bir zaman kaynağı ile uyumlu hale getirilmelidir.

f) Log analizine yardımcı olmak amacıyla, değişik log yapılarını tek bir standart ve tutarlı log yapısına dönüştürme yöntemleri kullanılmalıdır.

g) Loglar, 5651 sayılı kanun uyarınca iki yıl saklanmalıdır.

h) Loglar sistem ve ağ güvenliği ile ilgili bilgileri de içerebildiğinden, gizlilik ve bütünlük ihlallerine karşı korunmalıdır.

i) Logların güvenliği, sadece depolandıkları yerlerde değil, iletim esnasında da kasıtlı veya kasıtlı olmayan değişiklik ve tahribata karşı farklı ortamlarda da depolanması tercih edilmelidir.

j) Arşivlenen logların da gizlilik ve bütünlüğünün korunması sağlanmalıdır.

k) Log kaynak sistemlerinde, Bilgi İşlem Birimi personelleri haricinde, hiçbir personele okuma, yazma veya değişiklik amaçlı erişim izni verilmemelidir.

l) Log kayıtlarının üçüncü taraf kişi / kurumlar tarafından talep edilmesi durumunda, adli mercilerin verdiği karar doğrusunda log kayıtları ilgili kişi ya da adli mercilere teslim edilmelidir.

m) Sistemlerde tespit edilen anormallikler için Bilgi Güvenliği İhlal Prosedürü 'nde belirtilen yöntemlere göre aksiyon alınmalıdır.

n) Logların alınmaması durumları için otomatik uyarı sistemleri kurulmalıdır. Uyarı sisteminin kurulamadığı durumlarda belirli periyodlarda (en geç 2 haftada bir öngörülmektedir) loglar manuel kontrol edilmelidir.

o) Çok gizli ve özel nitelikli kişisel veri bulunan ortamlarda yapılan erişim, silme, kaydetme durumlarının log kayıtları alınmalıdır.

p) ALOTECH adına veri işleyen tedarikçi ya da alt taşeron olması durumunda; kişisel veri talepleri geldiği zaman sadece ilgili talebe ilişkin log kayıtlarını yetkili makamlarla paylaşmalıdır. Ölçülü veri paylaşımı esas alınmalıdır.

q) Log kayıtları üzerinde yetkisiz kişiler tarafından değişiklik yapmasının önüne geçilmesi ve kanıt niteliğinde olması için log kayıtlarına zaman damga vurulması tercih edilmelidir.

r) Çok gizli ve kişisel veri bulunan sistemlere ayrıcalıklı erişim sağlayan personel ve üçüncü taraf kişi / kurumların log kayıtları ya da ekran hareketlerinin görüntüsü alınmalıdır.

5.16. Güvenli Kodlama Kuralları

a) Geliştirme ortamı fiziksel ve mantıksal olarak yetkisiz erişime karşı korunmalı ve izole edilmelidir.
b) Yazılım geliştirme metodolojisinde güvenlik hususları sağlanmalıdır.
c) Tasarım aşamasında güvenlik gereksinimleri belirlenmeli ve dikkate alınmalıdır.
d) Proje aşamaları içinde güvenlik kontrol noktaları tespit edilmeli ve takip edilmelidir.
e) Güvenli veri depolarının kullanımına özen gösterilmelidir.
f) Değişiklikler izlenmeli ve versiyon kontrolünde güvenlik kontrolü dikkate alınmalıdır.
g) Geliştiriciler güvenlik açıklıklarından kaçınma, bulma ve onarma konusunda özen göstermelidir.
h) Yazılım geliştiricileri tarafından kullanılan kaynak kod yönetimi araçlarında mümkünse kriptolama kullanılmalıdır.
i) Geliştirme projelerinde güvenilir insan kaynağı çalıştırılmalıdır.
j) Geliştirme işlemlerine ait yedekler güvenli alanlarda saklanmalıdır.
k) Güvenli geliştirme ortamı için insan, süreç ve teknoloji odak alınarak riskler belirlenmeli ve gerekli önlemler alınmalıdır.
l) Güvenli kodlama standartları dikkate alınarak güvenli programlama teknikleri kullanılmalıdır.
m) Geliştiriciler güvenli kodlama standartları konusunda eğitilmeli, testler ve kod incelemeleriyle doğrulanmalıdır.