1. AMAÇ

Bilgi Güvenliği ve Kalite Yönetim Sistemi Politikalarının amacı Kurum personelinin, sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve kullanılabilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlerine karşı personelin ve kurumun haklarını korumaya adamıştır. Bilişim ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir güvenlik, bütün personellerin dâhil olduğu takım çalışmasıyla oluşturulabilir.

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. SORUMLULUKLAR

Politikanın hazırlanması ve güncellenmesi BGYS komisyonunun, uygulama onayı Genel Müdür Yardımcısı sorumluluğundadır.

4. TANIMLAR VE KISALTMALAR

BGYS: Bilgi Güvenliği Yönetim Sistemi

5. POLİTİKA

5.1. Kabul Edilebilir Kullanım Kuralları

a) ALOTECH İLETİŞİM TEKNOLOJİLERİ TİCARET A.Ş. 'nin gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Kurumun iş gereksinimi dışında bu bilgilerin kopyalanması ve iletilmesi yasaktır.
b) Kurum personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazların güvenliğini sağlamakla sorumludur. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.
c) Hiçbir personel, bilgisayarlarından antivirüs koruma yazılımını devre dışı bırakamaz.
d) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.
e) Bilgisayarlara hiçbir surette lisanssız program yüklenmemelidir.
f) Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmeli veya yetkili kişiler dışında erişilemeyecek alanlarda saklanmalıdır.
g) Bilgisayarlar üzerinden resmî belgeler, programlar ve eğitim belgeleri haricinde (müzik, film vb.) dosya alışverişinde bulunulmamalıdır.
h) Bilgisayarlarda oyun, eğlence vb. uygulamaların çalıştırılması ve kopyalanması yasaktır.

i) Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.
j) Herhangi bir kişi kendine ait olmayan kritik bir rapor bulur ise bu durumu Bilgi Güvenliği Yönetim Temsilcisi 'ne bildirmelidir.
k) "Gizli" kâğıt belgeleri kilitli ortamlarda muhafaza edilecektir.
l) Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez, saatler sistem tarafından otomatik olarak yönetilmektedir.
m) Laptop bilgisayarlar güvenlik açıklarına karşı korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda hemen Bilgi İşlem ile iletişime geçilmelidir.
n) Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer kurum bilgileri, yazılım lisansları vb. hakları kesinlikle ihlal edilmemelidir.
o) Kurum bilgileri kurum dışından üçüncü şahıslara iletilmemelidir.
p) Tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.
q) Kurum politika ve prosedürleri, İnsan Kaynakları ve ilgili yöneticiler tarafından Kurum personeline, yeni işe başlayanlara ve 3.taraflara duyurulacaktır. İlgili güvenlik politikalarına uyulacağı personel iş sözleşmesinde yer almalı ve personele imzalatılmalıdır.
r) ALOTECH bilgisayarlarında kişisel verilerin barındırılması yasaktır. ALOTECH ortamında tutulan ve iletilen tüm bilgiler ALOTECH 'in malıdır. ALOTECH bu bilgileri izleme ve denetleme hakkına sahiptir.
s) Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.
t) Hiçbir personel izin almadan kendi bilgisayarı veya başka bir kaynak kullanarak, ALOTECH 'in bilişim ağını tarayamaz, izleyemez veya dinleyemez.
u) Hiçbir personel, kurum içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.
v) Sosyal medya erişimi verilen kullanıcılar görevlerinin dışında bu haklarını kullanmaları yasaktır.
w) Sosyal medya üzerinden kurumu rencide edici, karalayıcı paylaşımlar yapılmamalıdır. Kurumun hassas bilgileri sosyal medya üzerinden paylaşılmamalıdır.

5.2. Temiz Masa Temiz Ekran Kuralları

a) Masa üzerinde kartvizit kutuları, kişisel ajandalar, değerli bilgilere sahip dokümanlar ile masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.
b) Kuruma ait kritik bilgi içeren dokümanlar başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.
c) Kısa süreli ayrılmalarda dahi, cep telefonu, taşınabilir bellek, harici hard disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.
d) Çalışma saatleri dışında dokümanların ve elektronik ortamların güvenliği için ofis kapılarının kilitli olmalıdır.
e) Müsvedde kâğıtların, kâğıt imha makinalarında kırpılarak imha edilmelidir.
f) Toplantı salonlarında gizli ve kritik bilgi içeren dokümanları toplantı sonrasında ilgili salonlarda bırakmamalı ve salonlardaki tahtalara alınmış notlar silinmelidir.

g) Fotokopi cihazlarının yetkisiz kullanılmamalı, cihaz belleğindeki kritik ve hassas bilgiler silinmelidir.
h) Hassas ve sınıflandırılmış bilgi içeren ortamlardaki bilgiler yazıcıdan çıktı alındıktan sonra hemen silinmelidir.
i) Bilgisayarların iş yapılmadığında kapatılmalı, parola kullanılarak korunmalı ve ekran açık kaldığında koruyucusunun otomatik olarak aktif hale getirilmelidir.
j) Personelin bilgisayarındaki, taşınabilir belleğindeki, harici diskteki ve benzeri depolama ortamlarındaki gizlilik dereceli bilgi içeren her türlü belgenin güvenliğini sağlamakla yükümlü olduğu ve taşınabilir bellek veya harici diske gizli veya önemli veri konulması gerekiyorsa kriptolayarak koruması gerekmektedir.
k) Personelin gizli belgeleri, parolaları, adresleri, özellikle taşınabilir bellek, e-posta, sosyal medya gibi alanlarda paylaşmamasına dikkat etmelidir, gerektiği ve bilinmeyen e-posta ve haber gruplarına üye olmamalıdır.
l) Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımdan sonra etkin yöntemler kullanılarak geri dönülmeyecek şekilde silinmelidir.
m) Elektronik posta ortamında kişisel parola bilgilerinin paylaşılmayacağı, parolaların gizli tutulacağı, kimse ile paylaşılmayacağı, yazılı olarak saklanmayacağı,
n) Kurum bilgisayarlarının personel haricinde yetkisiz kullanıcılara teslim edilmemelidir.
o) Kuruma ait işlerde ALOTECH İLETİŞİM TEKNOLOJİLERİ TİCARET A.Ş. e-posta adresi(@alotech.com.tr) kullanılmalıdır.

5.3. İnternet Kullanım Kuralları

a) Kurum bilgisayarları içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. Kurum kültürüne ve yasalara uygun olmayan siteler yasaklıdır. Ancak üst yönetimin yazılı izni ile yetkilendirilmiş kurum personeline internete çıkarken gerekli servisleri kullanma hakkı tanımlanmıştır. (FTP, sosyal medya)
b) 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az iki yıl arşivlenmektedir.
c) Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (film, müzik, program vb.) indirilmemelidir.
d) Tunnel platformları (VPN), proxy ve DNS değişiklikleri yapılarak internete bağlanılmamalıdır.
e) Başkalarının fikri haklarını ihlal edici materyal (yazı, makale, kitap, film, müzik eserleri vb.) dağıtılmamalıdır.
f) Sistem ve ağ güvenliğinin ihlal edilmesi cezai ve hukuki mesuliyetle sonuçlanabilir. ALOTECH bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa disiplin yönetmeliğini uygulayabilir veya yasa uygulayıcısı ile iş birliği yapabilir.
g) İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde mesajlar yayınlanmamalı ve paylaşılmamalıdır.
h) Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek online olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınlar kullanılmamalıdır.
i) ALOTECH e-posta adresi ile internet üzerinde forum, alışveriş vb. sitelere üye olunmamalıdır.
j) ALOTECH hesaplarına ait kullanıcı adı ve şifrenizin internet üzerinden paylaşılmamalıdır.

k) ALOTECH içerisinde kullanılan kullanıcı adı ve şifreleri ile sosyal hayatta kullanılan kullanıcı adı ve şifreleri aynı olmamalıdır.
l) İnternet üzerinden yaptığınız kişisel işlemlerinizde (banka, alışveriş, mail vb.) oluşacak olumsuzluklardan kurumumuz sorumlu değildir. Ayrıca, kurum veya kişisel hesabınızı ele geçiren kişi veya kişiler sizin adınıza suç işleyebilir, bu işlemden sorumlu olabilirsiniz.
m) İnternette gezinirken reklam veya bilgi çalmak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.
n) ALOTECH personelinin internete girmek için kendisine verilen wi-fi şifresini başkalarıyla paylaşmamalıdır.
o) ALOTECH network ağına kuruma ait olmayan cihazlar bağlanmamalıdır. Bu cihazların ALOTECH ağına bağlanması gereken durumlarda İdari birimine haber verilmelidir.

5.4. E-Posta Kullanım Kuralları

a) ALOTECH personelinin kurumsal e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar ALOTECH 'in bilgi varlığıdır. Bu yüzden yetkili kişiler gerekli durumlarda önceden haber vermeksizin e-posta mesajlarını denetleyebilir, yasal merciler ile paylaşabilir.

b) Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta ve ekleri virüs içerebilir. Kesinlikle ekler indirilmemeli veya açılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi İşlem Birimine veya Bilgi Güvenliği Ekibine haber verilmelidir. Yetkili kişiler müdahale edene kadar mesajın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

c) ALOTECH kurumsal e-posta hesapları kişisel amaçlar için kullanılmamalıdır.

d) ALOTECH e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine veya Bilgi Güvenliği Ekibine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.

e) Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.

f) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen Bilgi Güvenliği Ekibine haber verilmelidir.

g) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

h) Kullanıcıların kullanıcı kodu / şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal Bilgi Güvenliği Ekibine haber verilmelidir.

i) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

j) Kurum personeli kurumsal e-postaların herhangi bir kişi tarafından okunmamasını sağlamakla yükümlüdür.

k) ALOTECH mail hesabı kurulu olan cep telefonlarında ekran kilidi özelliği aktif olmalıdır.

5.5. Parola Kullanım Kuralları

a) Parolalar bilgisayar güvenliği için önemli bir özelliktir. Parolalar kompleks olmalıdır. Kolay tahmin edilen *(şehir, çocuk ismi, doğum tarihi, ardışık rakam ve harfler, İstanbul, İzmir, 1qaz2wsx, qwerty vb.)* parolalar kullanılmamalıdır.

b) ALOTECH içerisinde kullanılan genel kullanıcı bilgisayar şifreleri günde bir değiştirilmesi zorunlu kılınmıştır.

c) Oluşturulacak şifre son parola ile aynı olamaz.

d) Oluşturulacak parola içerisinde Türkçe karakter bulunmamalıdır.

e) Bilgisayar kullanıcı hesaplarının parolaları en az 8 karakter olmalıdır. Parola; büyük harf, küçük harf, rakam ve özel karakterden oluşmalıdır.

f) Kullanıcılar bilgisayar başından kalktığı zaman mutlaka oturumlarını kilitlemelidirler. *(Windows + L)* Genel kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 5 dakika içerisinde şifreli ekran korumasına girecektir.

g) Parola unutulması durumunda Bilgi İşlem Birimi ile iletişime geçilmelidir.

h) Kurumsal hesaplarınıza ait parolalarınız e-posta iletilerine, herhangi bir elektronik veya fiziksel bir ortama not alınmamalıdır.

i) Parola aile bireyleri dâhil kimseyle paylaşılmamalıdır.

j) Bir kullanıcı hesabı birden çok kişi tarafından kullanılmamalıdır.

k) Kişisel Verilerin Korunması Kanunu'na istinaden ALOTECH personelinin bizzat kendi talebi olmaksızın parolası sıfırlanamaz veya değiştirilemez.

l) Çok kritik veya kişisel verilerin üçüncü taraf kişi/kurumlar ile paylaşılması gereken durumlarda, bilgi şifrelenmeli ve şifre farklı bir yöntemle ilgili kişiye iletilmelidir.

5.6. Fiziksel Güvenlik Kuralları

a) 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 teşkil edilmelidir.

b) Ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.

c) Tanımlanan farklı güvenlik bölgelerine erişim yetkileri düzenli aralıklar ile kontrol edilmelidir.

d) Ofis girişleri ve koridorlar güvenlik açısından kamera ile kayıt altına alınmaktadır. Çalışma ortamlarının kapıları molalarda veya mesai bitimlerinde kapalı tutulmalıdır.

e) Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.

f) Özel veya kurumsal kargolar ofis asistanı tarafından teslim edilir. Kargonun sahibi ofis asitanından teslim alır.

g) Hasar / hırsızlık gibi oluşabilecek risklere karşı güvenlik sağlanmalıdır.

h) Ekipmanların kullanımı zimmetlenen kişiye aittir, bu ekipmanların güvenliğini sağlanması kişinin sorumluluğundadır.

i) ALOTECH dışına çıkarılan mobil cihazlar hırsızlık veya fiziksel hasara karşı uygun şekilde muhafaza edilmelidir.

j) Güvenlik kameraları ve diğer uygun güvenlik önlemleri kullanılarak tesislerdeki potansiyel fiziksel saldırılar aktif olarak gözetlenmelidir.

5.7. Kişisel Veri Güvenlik Kuralları

a) Kişisel veriler amacı dışında kullanılmamalıdır. İşin gereği kadar kişisel veriler, veri sahibinden talep edilmelidir. Elde edilen kişisel veriler bütünlüğü sağlayacak şekilde korunmalıdır.

b) Kişisel veriler kullanım amacı haricinde 3. Taraflar ile paylaşılmamalıdır.

c) Kişisel veriler, kurumun onaylamış olduğu imha yöntemleri ile yok edilmelidir. Kişisel verilerin saklama süreleri en geç 6 ayda bir kontrol edilmelidir.

d) ALOTECH'in sorumlu olduğu kişisel veriler hiçbir hukuki şart, sözleşme ya da yasal dayanak yoksa kurum dışından üçüncü şahıslara iletilmemelidir. ALOTECH'in sorumlu olduğu kişisel veriler (çalışanlar, müşteriler, tedarikçiler, acenteler vs.) ilgili kişinin izni olmadan 3. taraf kişiler ile paylaşılmamalıdır. Güvenilir kaynaklardan gelen talepler doğrultusunda işin gereği kadar veri paylaşılmalıdır.

e) Kişisel veriler 3.taraf kişi/kurumlara aktarılırken teknik ve idari tedbirleri alınmalıdır. 3. Taraflara kişisel veri aktarımında, kişisel veriler şifreli gönderilmelidir.

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

g) Ortak kullanılan cihazların (yazıcı, fax, fotokobi vb.) üzerinde kişisel veri barındıran belgeler bırakılmamalıdır.

h) Temiz Masa Temiz Ekran kurallarına uyulmalı, kişisel veri bulunduran basılı doküman ve bilgi depolayan medyalar (usb bellek, harici disk, cd vb.) masaların üzerinde bırakılmamalıdır.

i) Kişisel verilerin bulunduğu ortamlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

j) Aşağıda belirtilen hususların yaşanması durumunda ALOTECH İrtibat Kişisi aynı gün bilgilendirilmelidir;

k) Kişisel veri ihlâlinin gerçekleşmesi durumunda oluşması durumunda,

l) Kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde,

m) Kurum içinde ihlale sebebiyet verebilecek/verebilen açıklıkların oluşması durumunda,

n) Saklama süresi dolan verilere aksiyon alınması gereken durumlarda,

o) Kurum içi ve kurum dışı kişisel veri sahiplerinin, işlenen kişisel verileri hakkında talepleri Aydınlatma Beyanında (web sayfasında mevcut) belirtilen yöntemlere göre alınmalıdır.

p) Veri sahiplerinden gelen kişisel veri talepleri olumlu yada olumsuz en geç 30 gün içinde veri sahibine dönüş yapılmalıdır. Veri sahibi talebinin kabul edilmesi durumunda ise cevap dönülmesinden itibaren en geç 30 gün içerisinde aksiyon tamamlanmalıdır.

q) ALOTECH'in KVKK 'ya şikayet edilmesi durumunda en kısa sürede deliller toplanmalıdır. Talep ve şikayetlerin yönetimi için idari ve teknik tedbirlere göre uygun hareket edilmelidir.

r) Veri sahiplerinin kişisel verilerinin işlenmesi için açık rıza alınması gereken durumlarda, açık rıza alınmadan kişisel veriler kullanılmamalıdır.

s) Çalışanlar, birimlerinde yeni bir iş süreci oluşması ve/veya kişisel verilerin kullanma amaçlarının değişmesi durumunda, birim yöneticilerilerini ve ALOTECH İrtibat Kişisi'ni bilgilendirmelidir.

5.8. İmha Kuralları

a) Kişisel verilerin imhası gerçekleştirileceği zaman Kişisel Verilerin Korunması Politikası dikkate alınarak imhalar gerçekleştirilmeli ve gerçekleştirilen imhalar kayıt altına alınmalıdır.

b) Kişisel verilerden saklama süreleri dolan veri olup olmadığı en geç 6 ayda bir kontrol edilmelidir.

c) Elektronik cihazların imhasına karar verilmesi durumunda depolama alanları (hard disk) çıkartılarak bilgi işlem personeline teslim edilmelidir. Çıkartılan depolama alanları bilgi işlem personeli kontrolünde saklanmalıdır.

d) Saklanan ya da ihtiyaç duyulmayan donanımların imhası aşamasında İmha Tutanağı Formu kullanılmalıdır.

e) Gerek duyulması halinde atık hale gelen elektronik cihazlar Çevre ve Şehircilik Bakanlığı'ndan atık elektrikli ve elektronik eşya işleme konusunda lisansa sahip firmalar ile sözleşme yapılarak, imha işlemleri yapılabilir. Bu tarz durumlarda teslim edilen imha edilecek ürün bilgisi İmha Tutanağı Formu ile kayıt altına alınmalıdır.

f) İhtiyaç duyulmadığına karar verilen dokümanlar uygun metotlarla (kâğıt öğütücü, ince ince elde parçalanarak vb.) imha edilmelidir.

g) Gizli olarak tanımlanan (sözleşme, fatura, kişisel veri içeren, şartnameler, veri dokümanları vb.) dokümanlar ve kopyaları, müsvedde olarak kullanılmamalıdır. Hatalı çıktılar kâğıt öğütücü kullanılarak imha edilmeli ya da çıktı okunamayacak şekilde ince ince elle parçalanarak imha edilmelidir.

h) Kişisel veri barındırılan medyaların yeniden kullanılması gereken durumlarda, eski verilere tekrar erişimin engellenebilmesi için özel wipe (silme) uygulamaları kullanılmalıdır.

i) Bilgi sistemlerinde veya cihazlarda depolanan gereksiz bilgiler depolama süresi sona erdiğinde, güvenli bir şekilde silinmelidir.

5.9. Bilgi Transferi Kuralları

a) Üretilen veya elde edilen veri, ihtiyaca uygun olarak tasnif edilip belirli bir biçime kavuşturulduktan sonra çalışanların en kısa sürede ve kolay yoldan erişebilecekleri şekilde dağıtılmalı ve paylaşılmalıdır.

b) Bilgi transferleri e-mail ve Google Drive yollarıyla yapılmalıdır.
c) Bilgi transferlerinde bilgi türlerinin tanımlanmalı ve transfer boyutunun tespit edilmelidir.
d) Elektronik ortam yanı sıra; şirket kafetaryalarında, çay ocaklarında, servis araçlarında yapılan sohbetler, ev toplantıları veya çeşitli sosyal faaliyetlerde de istenmeyen bilgi transferine yönelik çalışanlara farkındalık ve uygulama eğitim programları düzenlenmelidir.
e) Bilgi transferinin kurum içi ve dışı olmasına göre açık ve örtülü güvenlik seviyeleri ile korunmalıdır.
f) Erişim Kontrol ve uzaktan erişim politikasında tanımlanan bilgi güvenliği kurallarına uyulmalıdır.
g) Bilgi transferine uygun ortamların güvenliği sağlanmalıdır.
h) Bilgi transferindeki uygun ortamın ofis, iş yeri vs. gibi fiziki, e-posta, telekonferans vs. gibi sanal olabileceği gibi tecrübelerin, fikirlerin ve ideallerin paylaşılması gibi zihni bir kavram da olabileceğinden hareketle; gerekli önlemlerin alınmalıdır.
i) Çalışanların kurum içi ve dışı bilgi transferindeki yetki ve sorumluluklarının tanımlanmalıdır.
j) Bilgi transferinde ortak iletişim dili olan Türkçe dili kullanılmalıdır.

5.10. Kriptografik Kontrol ve Anahtar Yönetimi Kuralları

a) Etkin kriptografik algoritmaları HMAC-SHA256 yönetimi kullanılır. Ayrıca Google tarafında bulundurulan datalar için AES-256 yöntemi kullanılmalıdır.
b) Standartlaştırılmış ve güvenli kriptografik algoritmalar içeren uygulama, cihaz ve sistemlerin kullanılmalıdır.
c) Kriptografik anahtarlar üretilirken ulusal ve uluslararası kabul görmüş anahtar uzunluklarının kullanılmalıdır.
d) Anahtar üretilirken tahmin edilebilir olmaması için komplike yapıda tasarlamalı.
e) Kriptografik anahtar revizyonu yapılması gereken durumların tanımlanması gerekir.
f) Anahtar üzerinde yapılan oluşturma, değişim, iptal gibi tüm iz kayıtlarının tutulmalıdır.
g) Kriptografik anahtarların amacına uygun yetkilendirilmelerinin yapılması gerekiyor.
h) Anahtarların üretildikten sonra kontrolsüz şekilde kopyalama ve çoğaltmanın engellenmesi gerekir.
i) Anahtarların tekil olarak kimlik adreslemesinin yapılması ve yaşam döngüsünün takip edilmesi gerekir.
j) Güvenli ağların güvensiz bir ağ üzerinden haberleşmesi durumunda VPN teknolojilerinin kullanılması gerekir.

5.11. Kalite Kuralları

a) Personellerimiz, ISO 9001 Kalite Yönetim Sistemi çerçevesinde kurumsal itibarımızı güçlendirmek ve şirket değerlerimizi güçlendirmek için çaba göstermeli ve bu yönde hareket etmelidir.

b) Kurumsal Performans ve Kurumsal Risk Yönetimi Sistemi oluşturulmalı ve periyodik olarak takibi yapılmalıdır. Gerekli aksiyonlar alınmalıdır.
c) Kurumsal hedeflere ulaşmak için personellerimiz etkin bir şekilde çalışmalı ve bu hedeflere ulaşmak için gerekli adımları atmaları gerekmektedir.
d) İş süreçlerimizi sürekli olarak iyileştirmek ve geliştirmek için personellerimiz gerekli önlemleri almalı ve aktif olarak katkıda bulunmalıdır.
e) Personellerimizin yetkinliğini artırmak için bireysel ve ekip çalışması eğitimlerine katılım göstermeleri gerekmektedir.
f) Müşterilerimizin, tedarikçilerimizin ve çalışanlarımızın memnuniyetini sağlamak için personellerimiz gereken özeni göstermeli ve gerekli adımları atmaları gerekmektedir.

5.12. Müşteri Memnuniyeti Kuralları

a) Müşterilerimizin ihtiyaç ve beklentileri açık, şeffaf, hızlı, güven verici ve müşteri odaklı bir şekilde, kaliteli hizmet sunma anlayışıyla ele alınmalıdır.

b) Müşterilerimizin bize ihtiyaçlarını kolaylıkla iletebilmesi için gerekli altyapı sürekli erişebilir tutulmalıdır.

c) Müşteri memnuniyet anketleri ile geri bildirimler doğrudan toplanmalı ve analizleri yapılmalıdır.

d) Müşterilere anında ve hızlı çözümle geri dönüş yapılmalıdır.

e) Müşterilerden gelen tüm bildirimlere açık olunmalı ve bu bildirimler objektif bir şekilde, şeffaflık, erişilebilirlik, gizlilik ve güvenilirlik ilkelerine uygun olarak çözüme ulaştırılmalıdır. Bu bilgiler etkin şekilde kontrol altında tutulmalıdır.

f) Müşteri ihtiyaç ve beklentileri, şikayet ve önerilere dayalı çözümler kalıcı hale getirilerek müşteri memnuniyeti sistemleri sürekli olarak iyileştirilmelidir.

g) Sürekli iyileştirme ve geliştirme felsefesi tüm süreçlere etkin şekilde entegre edilmelidir.

h) Müşteri beklentileri, yasal mevzuat ve standartlara uygun çözümler üretilmelidir.

i) Müşteri Memnuniyeti Politikası, şirketin tüm çalışanlarına anlatılmalı, benimsetilmeli, sahiplenilmeli ve sürekliliği sağlanmalıdır.

j) Satış öncesinde ve satış sonrasında tüm süreçler müşteri odaklı bir yaklaşımla gerçekleştirilmelidir.

k) Müşterilere sunulan ürün veya hizmetler için güçlü, doğru, net ve devamlılık sağlayan müşteri-kurum ilişkisi oluşturulmalıdır.

5.13. İş Sürekliliği Kuralları

a) Afet ve acil durumlarda birinci öncelik olarak can güvenliğini sağlanmalıdır.
b) İş sürekliliğini sağlamak amacıyla tüm fiziksel ve elektronik bilgi varlıkları en etkin şekilde kullanılmalıdır.

c) İş-etki analizleri düzenli periyotlarla gerçekleştirilmeli ve sonuçlarına göre önleyici ve koruyucu tedbirler alınmalıdır.
d) Önem derecesi yüksek varlıkların Risk Değerlendirme ve Risk İşleme çalışmaları yapılarak gereken tedbirler alınmalıdır.
e) Konuşma, mesajlaşma, internet ve toplumsal güvenlik hizmetlerinin sürekliliği sağlanmalıdır.
f) İş sürekliliği yönetimi kapasitesi sürekli olarak iyileştirilmelidir.
g) Güvenilir, itibarlı ve sağlam firma imajı korunarak çalışmalar devam ettirilmelidir.
h) İş sürekliliğinin sağlanması ile şirketin itibar ve marka değeri korunmalıdır.
i) İş sürekliliği için Bilgi ve İletişim Teknoloji hedefleri belirlenmeli, planlanmalı, sürdürülmeli ve düzenli olarak test edilmelidir.

KULLANICI POLİTİKALARI KABUL ONAYI

Kurum Yönetim Sistemi Politikalarında ifade edilen tüm kurallara uymayı, iş bu güvenlik politikalarının ve revizyonlarının Bilgi Güvenliği ve Kalite Yönetim Sistemi'nde yayınlandığını bildiğinizi ve güncellemeleri takip ederek iş bu değişikliklere uygun davranacağınızı aksi takdirde hakkınızda disiplin ve yasal her türlü işlemin başlatılacağını bildiğinizi kabul ve taahhüt etmektesiniz.

İzlenecek Prosedür

1. Kullanıcı Politikalarını okuyunuz.

2. Aşağıdaki belirtilen bölümlere bilgileri doldurup imzalayınız.

3. Bu sayfayı İnsan Kaynakları Birimine teslim ediniz.

Kullanıcı Taahhüdü

Bu forma imza atarak Kullanıcı Politikalarında yazan kurallara uyacağımı taahhüt ediyorum.

ALOTECH İLETİŞİM TEKNOLOJİLERİ TİCARET A.Ş Kullanıcı Politikalarının kabul onayının bir kopyasını teslim aldım, okudum ve anladım.

Personelin;

İmza :

T.C. Kimlik/Pasaport No :

Ad ve Soyad :

Unvan :

Bölüm :

Tarih :