TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

ÖZET

Bilgi Güvenliği Yönetim Sistemi Politikalarının amacı TÜMAD Madencilik Sanayi ve Ticaret A.Ş. personelinin, sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.
TÜMAD'ın amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. TÜMAD bilerek veya bilmeyerek yapılan yasadışı veya zararlı eylemlerine karşı çalışanların ve TÜMAD'ın haklarını korumaya adamıştır. Bilişim ile alakalı sistemler TÜMAD'ın sahip olduğu değerlerdir. Güçlü bir güvenlik bütün çalışanların içerisine dahil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.
BGYS politikalarının, gözden geçirilmesi ve güncellenmesinden BGYS Yönetim Temsilcisi ve BGYS Ekibi sorumludur. TÜMAD Madencilik San. ve Tic. A.Ş. Yönetimi, Bilgi Güvenliği Politikasını onaylar ve duyurulmasını sağlar. Bu politikalara uyulmasından iç ve dış tüm ilgililer sorumludur.

Yaptırım
Bu politikalara uygun olarak hareket etmeyen tüm personel hakkında İnsan Kaynakları Disiplin Prosedürü (TMD_IK_PRD.004) uygulanır.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

BİLGİ GÜVENLİĞİ GENEL POLİTİKASI

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. bünyesinde bulunan maden arama ruhsatlarında değerli ve baz metaller konusunda projeleri ve aramaları olan, altın üretimi gerçekleştiren bir Türk madencilik grubudur.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. ISO 27001:2013 Bilgi Güvenliği Yönetim Sistem Standardı doğrultusunda;

- Kendisi ve paydaşlarının bilgi varlıklarına güvenli bir şekilde erişim sağlamayı,
- Bilginin kullanılabilirliğini, bütünlüğünü ve gizliliğini korumayı,
- Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,
- TÜMAD'ın güvenilirliğini ve marka imajını korumayı,
- Bilgi güvenliği ihlali durumunda gerekli görülen yaptırımları uygulamayı,
- Tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, ilgili mevzuat ve standart gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimlerini sağlamayı,
- İş/hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı, işin sürekliliğini ve sürdürülebilirliğini sağlamayı,
- Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi,
- Bilgi güvenliği farkındalığını arttırmak amacıyla yetkinlikleri geliştirecek eğitimleri sağlamayı,

Taahhüt eder.

Hasan YÜCEL
Genel Müdür

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

İNTERNET ERİŞİM POLİTİKASI

TÜMAD içinde güvenli internet erişimi için sahip olması gereken standartların belirlenmesi gerekmektedir. İnternetin uygun olmayan kullanımı, TÜMAD'ın yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeyerek bu türden olumsuzluklara neden olunmaması ve internetin kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır. Bu politika TÜMAD AŞ'nin internetini kullanan tüm çalışanları kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. İnternet Erişim Politikası doğrultusunda;

- TÜMAD bilgisayarları içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. TÜMAD kültürüne ve yasalara uygun olmayan siteler yasaklıdır. Ancak üst yönetimin yazılı izni ile yetkilendirilmiş TÜMAD personeline internete çıkarken gerekli servisleri kullanma hakkı tanımlanmıştır.
- 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği TÜMAD'ın internet erişim kayıtları en az 2 yıl arşivlenmektedir.
- Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (film, müzik, program vb.) indirmek yasaktır.
- Tunnel platformları, proxy ve dns değişiklikleri yapılarak internete bağlanılması yasaktır.
- Başkalarının fikri haklarını ihlal edici mahiyette (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.
- Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. TÜMAD bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa disiplin yönetmeliğini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.
- İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde mesajlar yayınlamak ve paylaşmak yasaktır.
- Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek online olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınların kullanılması yasaktır.
- TÜMAD mail adresi ile internet üzerinde forum, alışveriş vb. sitelere üye olunması yasaktır.
- TÜMAD hesaplarına ait kullanıcı adı ve şifrelerin internet üzerinden paylaşılması yasaktır.
- TÜMAD içerisinde kullanılan kullanıcı adı ve şifreler ile sosyal hayatta kullanılan kullanıcı adı ve şifreler aynı olmamalıdır.
- İnternet üzerinden yaptığınız kişisel işlemlerinizde (banka, alışveriş, mail vb.) oluşacak olumsuzluklardan TÜMAD sorumlu değildir. Ayrıca, şirket veya kişisel hesabınızı ele geçiren kişi veya kişiler sizin adınıza suç işleyebilir, bu işlemden mesul olabilirsiniz.
- İnternette gezinirken reklam veya bilgi çalmak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.
- 3. Şahıs internet erişimi için kablosuz ziyaretçi ağına bağlanacaktır. Ziyaretçi bu sisteme bağlanabilmek için gerekli kişisel bilgilerini girerek kendi kayıt işlemini sağlamak zorundadır. Bir sonraki ziyaretinde bu işlemi tekrarlaması gerekir.
- TÜMAD personelinin internete girmek için kendisine verilen TÜMAD kimliği ve şifresini başkalarıyla paylaşması yasaktır.
- TÜMAD network ağına TÜMAD dışı cihazların takılması yasaktır.

TÜMAD

MADENCİLİK SANAYİ VE TİCARET A.Ş.

E-POSTA POLİTİKASI

Bu politikanın amacı TÜMAD Madencilik Sanayi ve Ticaret A.Ş. e-posta altyapısına yönelik kuralları ortaya koymaktır. TÜMAD' ta oluşturulan e-postalar resmi bir kimlik taşımaktadırlar. E-posta TÜMAD' in en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta erişim kolaylığı ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır. Bu politika TÜMAD e-postasını kullanan tüm çalışanları kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. E- Posta Politikası doğrultusunda;

- TÜMAD çalışanlarının, TÜMAD e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar TÜMAD bilgi varlığıdır. Bu yüzden yetkili kişiler gerekli durumlarda önceden haber vermeksizin e-posta mesajlarını denetleyebilir, yasal merciler ile paylaşabilir.
- Personel e-posta adresi isim soyisim olacak şeklinde açılmaktadır. Örnek: Bilge KÜÇÜKAYTAN isimli personel için; bilge.kucukaytan@tumad.com.tr olacak şekilde mail hesabı açılır. Benzer isim olması durumunda e-posta belirleme talimatına göre kurulum işlemi gerçekleştirilir.
- Şirket e-posta hesapları kişisel amaçlar için kullanılmamalıdır.
- Kişisel kullanım için internetteki sitelere üye olunması durumunda TÜMAD e-posta adresleri kullanılmamalıdır.
- TÜMAD'ın e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen Bilgi İşlem Bölümü'ne haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemelidir. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt verilmemelidir.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal Bilgi İşlem Bölümü'ne haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.
- Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve konuyla ilgili Bilgi İşlem Bölümü'ne haber verilmelidir.
- TÜMAD çalışanları, TÜMAD e-postalarının herhangi bir kişi tarafından okunmamasını sağlamakla yükümlüdür.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

ANTİ-VİRÜS POLİTİKASI

Bu politika ile TÜMAD Madencilik A.Ş'de bilgisayar ve sunucuların zararlı yazılımlardan korunması amaçlanmaktadır. Bu politika TÜMAD Madencilik A.Ş 'de bulunan bilgisayarları ve sunucuları kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Anti-Virüs Politikası doğrultusunda;

- TÜMAD'ın bütün bilgisayarları ve sunucuları anti-virüs yazılımına sahip olmalıdır.
- Düzenli aralıklar ile anti-virüs yazılımı otomatik olarak güncellenmelidir.
- Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmamalıdır.
- Kullanıcı herhangi bir sebepten dolayı anti-virüs programını sistemden kaldıramaz veya durduramaz.
- Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta ve ekleri virüs içerebilir. Kesinlikle açılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında hemen Bilgi İşlem Bölümü'ne haber verilmesi ve yetkili kişiler müdahale edene kadar mesajın silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.
- Bilinmeyen ve şüpheli kaynaklardan indirilen dosyaların içerisinde virüs olabilir. Bu tür kaynaklardan dosya indirilmesi yasaktır.
- Bilgisayarlarda kullanılan CD, USB, Harici Disk gibi depolama aygıtları virüs taraması yapılmadan kullanılmamalıdır.
- TÜMAD dışı CD, USB, Harici Disk vb. materyaller TÜMAD bilgisayarlarına takılması yasaktır. Oluşabilecek her türlü olumsuzluklardan personel sorumludur.
- TÜMAD ağına antivirüs yüklü ve güncel olmayan bilgisayarlar dahil edilmemelidir.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

ŞİFRE POLİTİKASI

Bu politika ile güçlü bir şifreleme oluşturulması ve şifrelerin güvenliğinin sağlanması amaçlanmaktadır. Bilgisayarları ve sunucuları kullanan bütün kullanıcı hesaplarını kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Şifre Politikası doğrultusunda;

- Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Şifreler kompleks olmalıdır. Sistem tarafından İsim Soyisim içeren şifreler kabul edilmemektedir. Ayrıca son 5 şifrenin tekrar kullanılmasını kabul etmez. Kolay tahmin edilen (memleket, çocuk, doğum tarihi, ardışık rakam ve harfler, vb.) şifreler (İstanbul, Ankara, 1qaz2wsx, qwerty vb.) kullanılmamalıdır.
- TÜMAD içerisinde kullanılan genel kullanıcı bilgisayar şifreleri 45 günde bir değiştirilmesi zorunlu kılınmıştır.
- Bilgisayar kullanıcı hesaplarının şifreleri en az 8 karakter olmalıdır. Kompleks şifre içeriğinde; büyük harf, küçük harf, rakam, özel karakter seçeneklerinden oluşması gerekmektedir.
- Kullanıcılar bilgisayar başından kalktığı zaman mutlaka oturumlarını kilitlemelidirler (⊞ + L). Genel kullanıcı bilgisayarları, kullanılmadığı zaman otomatik olarak 5 dakika içerisinde şifreli ekran korumasına girecektir.
- 3 kez üst üste şifrenin hatalı girilmesi sistemin kilitlenmesine sebep olmaktadır. Şifrenin unutulması durumunda Bilgi İşlem Bölümü ile iletişime geçilmelidir.
- TÜMAD hesaplarınıza ait şifrelerinizin e-posta iletilerine veya herhangi bir elektronik forma yazılması yasaktır.
- Şifre bilgilerinin aile bireyleri dahil kimseyle paylaşılması, kağıtlara ya da elektronik ortamlara yazılması yasaktır.
- Bilgi İşlem Bölümü tarafından size oluşturulan yeni şifreleri hemen değiştirmeniz gerekmektedir.
- Bir kullanıcı hesabı birden çok kişi tarafından kullanılmamalıdır.
- Kişisel Verilerin Korunması Kanunu'na istinaden aktif TÜMAD personelinin bizzat kendi talebi olmaksızın şifresi sıfırlanamaz veya değiştirilemez.

TÜMAD

MADENCİLİK SANAYİ VE TİCARET A.Ş.

FİZİKSEL GÜVENLİK POLİTİKASI

Bu politika ile TÜMAD personeli ve kritik TÜMAD bilgilerinin korunması amacıyla sistem odasına, TÜMAD bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve TÜMAD binalarına yetkisiz girişlerin önlenmesi amaçlanmaktadır.
TÜMAD binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Fiziksel Güvenlik Politikası doğrultusunda;

- TÜMAD 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 alt yapıları teşkil edilmelidir.
- TÜMAD dışı ziyaretçilerin ve yetkisiz personelin güvenli alanlara girişi yetkili görevliler gözetiminde gerçekleştirilmelidir.
- Tanımlanan farklı güvenlik bölgelerine erişim yetkilerinin düzenli aralıklar ile kontrol edilmelidir.
- Ofis girişleri ve koridorlar güvenlik açısından kamera ile kayıt altına alınmalıdır.
- Kritik sistemler özel sistem odalarında tutulmalıdır.
- Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalıdır.
- Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.
- Bireysel kargolar, İdari İşler Bölümünce belirlenen noktalarda yetkili kişiler tarafından teslim alınacaktır. Kargo çalışanlarının merkez ofis ve işletmelerin içine girilmesine müsaade edilmeyecektir.
- Ekipmanların kullanımı zimmetlenen kişiye aittir, bu ekipmanların güvenliğinin sağlanması kişinin sorumluluğundadır.
- Gelen ziyaretçiden kimlik ibraz edilerek kayıt yapılmalıdır.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

SUNUCU GÜVENLİK POLİTİKASI

Bu politika ile TÜMAD'ın sahip olduğu sunucuların temel güvenlik kurallarını oluşturmayı amaçlamaktadır.

Bu politika TÜMAD'ın sahip olduğu bütün sunucuları kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Sunucu Güvenlik Politikası doğrultusunda;

- TÜMAD bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.
- Bütün sunucular (TÜMAD'ın sahip olduğu) ilgili envanter yönetim sistemine kayıtlı olmalıdır.
- Sunucu işletim sistemleri üzerindeki kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- Kullanılmayan sunucular güvenlik ve elektrik tasarrufu açısından kapalı tutulmalıdır.
- Sunucular üzerinde yapılan işlemlerin log kayıtları en az 1 ay saklanacak şekilde ayarlanmalıdır.
- Sunucuların yönetimi için her sunucunun kendi hesabı ile bağlantı yapılmalıdır.
- Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulunmalıdırlar.
- Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenmelidir.
- Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt altına alınmalıdır. Sistem odası sunucu bakımları refakatçi kontrolünde olmalıdır.
- Elektrik ve data kabloları sunucu odaları dahil TÜMAD'ın içerisinde ayrı kanallardan geçmelidir.
- Sunucu odalarındaki ekipman bakımları düzenli olarak yapılmalı ve bakım kayıtları tutulmalıdır.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

AĞ YÖNETİMİ POLİTİKASI

Bu politika ile TÜMAD bilgisayar ağında yer alan bilgilerin, ağ alt yapısının, ekipmanların güvenliğinin ve sürekliliğinin sağlanması amaçlanmaktadır.

TÜMAD bünyesindeki ağ altyapısı, ekipman ve kullanıcıları kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Sunucu Ağ Yönetimi Politikası doğrultusunda;

- Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedekli ekipman bulundurulmalı.
- Ağ ekipmanları sadece yetkilendirilmiş kişiler tarafından erişilebilir ve yönetilebilir olmalıdır. Yetkisiz erişime karşı korunmalıdır.
- TÜMAD ağına sadece TÜMAD bilgisayarları bağlanmalıdır. TÜMAD dışında bir bilgisayar bağlanacak ise yetkili kişinin izni ve gözetiminde bağlanmalıdır.
- TÜMAD internet ağına misafirler alınmamalı, misafir ağı TÜMAD ağından bağımsız tasarlanmalıdır.
- Kamera, IP Santral, Kablosuz ağ ve kullanıcı ağları birbirinden ayrı olmalıdır.
- Ağ cihazları yılda en az 1 defa açıklık tarama testlerinden geçirilerek güvenli hale getirilmelidir.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

TEDARİKÇİ VE ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

Bu politika ile TÜMAD'ın bilgi sistemlerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlanması amaçlanmaktadır.
Bu politikanın uygulanmasından tüm departmanlar sorumludur.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Sunucu Tedarikçi ve Üçüncü Taraf Güvenlik Politikası doğrultusunda;

- Tedarikçiler, bakım firmaları veya üçüncü taraflar (müşteriler) bilgi sistemlerimize veya bilgi varlıklarımıza bakım vb. amaç ile geldiklerinde Gizlilik Anlaşması yapılması gerekmektedir.
- TÜMAD içerisinde bulundukları sürece TÜMAD politikalarına uygun hareket etmekle yükümlüdürler.
- Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerinde veya bilgi varlıkları üzerinde yapacakları çalışmaları Bilgi Güvenliği Yönetim Temsilcisine bildirilmelidir.
- Tedarikçiler, bakım firmaları veya üçüncü taraflara verilen fiziksel erişim yetkileri, erişim amaçlarına uygun olarak sadece çalışma alanlarında olacak şekilde kısıtlı verilmelidir.
- Tedarikçiler, bakım firmaları veya üçüncü taraflar bilgi sistemlerine ve bilgi varlıklarına fiziksel olarak eriştikleri süre boyunca refakatçisiz bırakılmamalıdır.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Bu politika, personelin sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarını bildirmeyi amaçlamaktadır.
Bu politika TÜMAD bünyesindeki tüm çalışanları kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Kabul Edilebilir Kullanım Politikası doğrultusunda;

- TÜMAD Madencilik Sanayi ve Ticaret A.Ş.'nin gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. TÜMAD'ın iş gereksinimi dışında bu bilgilerin kopya edilmesi ve iletilmesi yasaktır.
- TÜMAD Madencilik Sanayi ve Ticaret A.Ş. personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazların güvenliğini korumakla yükümlüdür. Erişim bilgileri başkaları ile paylaşılamaz.
- Hiçbir personel, bilgisayarlarından anti virüs koruma yazılımını devre dışı bırakamaz.
- Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.
- Bilgisayarlara lisanssız program yüklenmemelidir.
- Kullanıcı herhangi bir bilginin çok kritik olduğunu düşünüyorsa o bilgi şifrelenmeli veya yetkili kişiler dışında erişilemeyecek alanlarda saklanmalıdır.
- Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde (müzik, film vb.) dosya alışverişinde bulunulmamalıdır.
- Bilgisayarlarda oyun, eğlence vb. uygulamaların çalıştırılması ve kopyalanması yasaktır.
- Kritik raporların dökümünü alan kullanıcı, rapor içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.
- Herhangi bir kişi kendine ait olmayan kritik bir rapor bulur ise bu durumu Bilgi Güvenliği Yönetim Temsilcisi'ne bildirmelidir.
- "Gizli" kağıt belgeleri kilitli dolaplarda muhafaza edilecektir.
- Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez, sunucu saati ile bilgisayar saati arasında 5 dakikadan fazla fark var ise kullanıcı oturumuna sistem müsaade etmez.
- Dizüstü bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda hemen Bilgi İşlem Bölümü ile iletişime geçilmelidir.
- Herhangi bir kişi veya TÜMAD' tan izinsiz kopyalama, ticari sır, patent veya diğer şirket bilgileri, yazılım lisansları vb. hakları kesinlikle ihlal edilmemelidir.
- TÜMAD bilgileri, TÜMAD dışından üçüncü şahıslara iletilmemelidir.
- Tüm personel, kendi alanlarına ait Güvenlik Politikalarına uymak zorundadır.
- TÜMAD politika ve prosedürleri, İnsan Kaynakları ve ilgili yöneticiler tarafından TÜMAD çalışanlarına, yeni işe başlayanlara ve müşterilere duyurulacaktır. İlgili Güvenlik Politikalarına uyulacağı personel iş sözleşmesinde yer almalı ve personele imzalatılmalıdır.
- TÜMAD bilgisayarlarında kişisel verilerin barındırılması yasaktır. TÜMAD şirket ortamında tutulan ve iletilen tüm bilgiler şirketin malıdır ve TÜMAD bu bilgileri izleme ve denetleme hakkına sahiptir.
- Kaynağı belli olmayan ve üretici firması tarafından kopya edilmesi yasaklanmış bir bilgisayar yazılımını kopyalamak yasaktır.
- Hiçbir personel izin almadan kendi PC' sinden veya başka bir kaynak kullanarak, TÜMAD'ın Bilişim Ağını tarayamaz, izleyemez veya dinleyemez.
- Hiçbir personel, şirket içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.
- Sosyal medya üzerinden rencide edici, karalayıcı paylaşımlar yapılmamalıdır. TÜMAD ile ilgili hassas fotoğraf ve bilgiler sosyal medya üzerinden paylaşılamaz.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

TEMİZ MASA TEMİZ EKRAN POLİTİKASI

Bu politika, çalışanların mesai saatleri içi veya dışında kendilerine görevleri gereği paylaşılmış olan bilgilerin yetkisiz erişimler veya uygunsuz kullanımı sonucunda başına gelebilecek riskleri ortadan kaldırmayı amaçlamaktadır.
Bu politika; Çalışma masalarını ekranları, basılı dokümanları, belgeleri ve kayıtları kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Temiz Masa Temiz Ekran Politikası doğrultusunda;

- Çalışma sonunda kağıt ortamında ya da elektronik cihazlar üzerinde tutulan "gizli ya da çok gizli" bilgiler güvenlikli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklanacaktır.
- Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) yetkisiz erişimlere bırakılmayacaktır. Cihazlar üzerinde belge, doküman bırakılmayacaktır.
- Her türlü ekrandan ulaşılabilen bilgiler, şifreler, anahtarlar ve kodlar, bilginin sunulduğu sistemler, ana makineler (sunucu), PC'ler vb. cihazlar şifresiz kullanılmayacaktır.
- Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası vb. hassas bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.
- Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), Bilgisayarlar vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.
- Faks ve fotokopi makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır.
- Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale gelmesinin önüne geçilmelidir.
- Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem + L tuşuna basılarak yapılabilir.
- Bilgisayarların masaüstlerindeki klasör ve dosyalar düzenli tutulmalıdır.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

MOBİL VE TAŞINABİLİR CİHAZ POLİTİKASI

Bu politikanın amacı TÜMAD'a ait bilgi içeren mobil ve taşınabilir cihazların kullanımı ile ilgili kuralları belirlemektir.

Bu politikanın uygulanmasından mobil ve taşınabilir cihaz kullanan tüm çalışanlar sorumludur.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Mobil ve Taşınabilir Cihaz Politikası doğrultusunda;

- Kuruluşa ait bilgi içeren taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.
- Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
- Etki alanı dahilindeki bilgisayarlar admin yetkisi sınırlandırılarak yalnızca User yetkilendirmesi ile ilgili kişiye teslim edilmelidir.
- Taşınabilir cihazlara, yetkisiz erişime karşı şifre tanımlanmalıdır.
- Etki alanı dahilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar departmanlara ait ilgili ortak alana kaydedilmelidir.
- Taşınabilir cihazlar, aile bireyleri dâhil yetki dışı hiç kimse tarafından kullandırılmamalıdır.
- Taşınabilir cihazlar, görüntüleme aygıtları (fotoğraf makinası, video kamera) vb. cihazlarda ne tür bilgiler sakladığınızın farkında olun, hassas ve gizli bilgileri mümkün olduğunca mobil cihazlarda bulundurulmamalıdır.
- Kaybolması ve çalınması kolay olduğundan taşınabilir cihazlar başıboş bırakılmamalıdır.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

DEĞİŞİM YÖNETİMİ POLİTİKASI

Bu politika ile TÜMAD'ın bilgi sistemlerinde yapılması gereken yazılımsal ve donanımsal değişikliklerinin güvenlik ve sistem sürekliliğini aksatmayacak şekilde yürütülmesini amaçlamaktadır.
Tüm bilgi sistemleri ve bu sistemlerin işletilmesinden sorumlu personel bu politikanın kapsamında yer almaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Değişim Yönetimi Politikası doğrultusunda;

- Yazılımsal ve donanımsal değişiklikler kayıt altında tutulmalıdır.
- Bilgi sistemlerinde değişiklik yetkilendirilmiş kişiler tarafından yapılmalıdır.
- Herhangi bir sistemde uzun süreli veya önemli değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve ilgili kişilere bilgi verilmelidir.
- Değişiklikler gerçekleştirilmeden önce TÜMAD'ın ilgili birimine bilgi verilmelidir.
- Yapılacak değişiklikten önce değişikliğin yapılacağı sistemlerin yedekleri alınmalıdır.
- Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticilere bilgi verilmelidir.
- Yapılacak değişiklikler mümkün olduğunca test sunucuları üzerinde gerçekleştirilmelidir, yapılan testlerin başarılı geçmesi halinde canlı sistemde değişiklik gerçekleştirilmelidir.
- Değişikliğin varlık kritikliğine göre yapılacağı zaman ve yöntemler, işlemi yapacak bilgi işlem personeli tarafından yönetime bildirmelidir.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

Bu politikanın amacı; TÜMAD'ın bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarını tanımlamaktır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. bilgi sistemlerine erişen TÜMAD personeli ile TÜMAD dışı kullanıcılar bu politika kapsamı altındadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Kimlik Doğrulama ve Yetkilendirme Politikası doğrultusunda;

- TÜMAD sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.
- TÜMAD bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, işletim sistemleri ve log-on olarak erişilen sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, denetim altında tutulmalıdır.
- Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
- Kullanıcılar da TÜMAD tarafından kullanımlarına tahsis edilen sistemlerin güvenliğinden sorumludur.
- Sistemlerin başarılı ve başarısız erişim logları düzenli olarak tutulmalıdır.
- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve kayıt alınmalıdır.
- Kullanıcı hatalarını izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

TÜMAD

MADENCİLİK SANAYİ VE TİCARET A.Ş.

KRİPTOGRAFİK KONTROLLER POLİTİKASI

Bu politika ile bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunması amaçlanmaktadır. Bu politika bilgi varlıklarının saklandığı sistemler ve o sistemlere erişimin yapıldığı ağların şifre politikasını kapsamaktadır.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Kriptografik Kontroller Politikası doğrultusunda;

- TÜMAD içerisinde tanımlanan gizli bilgi varlıkları kriptografik şifreleme yöntemleri ile saklanmalıdır. Her personel kendi barındırdığı bilgi varlıklarının güvenliğinden sorumludur.
- Risk değerlendirmelerine göre yüksek düzeyde koruma gerektiren bilgi varlıklarının korunmasında güçlü şifreleme algoritması kullanılmalıdır.
- Tanımlanan şifreler belirli aralıklarla değiştirilmelidir.
- Active Directory hesap şifreleri kolay tahmin edilmeyen karmaşık şifreler olmalıdır.

TÜMAD

MADENCİLİK SANAYİ VE TİCARET A.Ş.

ZİYARETÇİ KABUL POLİTİKASI

Bu politikanın amacı dışarıdan gelen misafirlerin kabulü, kuruluş içinde dolaşmaları ve kuruluştan uğurlanmaları ile ilgili kuralları belirlemektir.

Bu politikanın uygulanmasından TÜMAD Madencilik Sanayi ve Ticaret A.Ş. deki tüm yönetici ve çalışanlar sorumludur.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Ziyaretçi Kabul Politikası doğrultusunda;

- Dışarıdan ziyaret amaçlı gelen kişiler/araçlar kuruluş girişinde güvenlik tarafından karşılanır, kimlik/araç ruhsatı alındıktan ve ilgili birim veya kişi ile irtibata geçildikten sonra güvenlik personelinin refakatiyle girişine izin verilir.
- TÜMAD içine gelen ziyaretçiler kamera sistemi ile takip edilmelidir. Ziyaretçilerin izinsiz girişlerine müsaade edilmemelidir.
- Kritik birimlere yetkisiz ziyaret girişlerini kısıtlamak için fiziki güvenlik önlemleri alınmalıdır.
- Ziyaretçiler internet kullanmak istediklerinde sadece Yönetim Misafir kablosuz internet ağını kullanabilirler.
- Bu politikaya uygun olarak çalışmayan tüm personel hakkında İnsan Kaynakları Disiplin Prosedürün (TMD_IK_PRD.004) de belirtilen maddeler uygulanır.
- Gelen ziyaretçilerin giriş-çıkış saatleri ve bilgileri kaydedilmektedir.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

OLAY İHLAL BİLDİRİM VE YÖNETİM POLİTİKASI

Bu politikanın amacı TÜMAD Madencilik Sanayi ve Ticaret A.Ş'nin bilgi güvenliği olay ihlal süreçlerini belirlemektir.
Bu politikanın uygulanmasından tüm personel sorumludur.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Olay İhlal Bildirim ve Yönetim Politikası doğrultusunda;

- Bilginin gizlilik, bütünlük ve kullanılabilirlik 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.
- Bilgi güvenliği olay raporlarının bildirilmesini, işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir geri besleme süreci oluşturulmalıdır.
- Bilgi güvenliği ihlali oluşması durumunda, kişilerin tüm gerekli faaliyetleri değerlendirmesi Bilgi Güvenliği Ekibi ile birlikte yapılmalıdır.
- İhlali yapan kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
- Tüm çalışanlar, üçüncü taraf kullanıcıları ve sözleşme tarafları bilgi güvenliği ihlallerini önlemek maksadıyla güvenlik zayıflıklarını doğrudan kendi yönetimlerine ve Bilgi Güvenliği Ekibine mümkün olan en kısa sürede rapor vermelidir.
- 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 alınır.
- İç problem analizi, adli incelemeler veya üretici firmadan zararın telafi edilmesi için aynı türdeki olayların izleme kayıtları (log) toplanır ve korunur.
- Güvenlik ihlallerinden kurtulmak için gereken eylemler, sistem hatalarının düzeltilmesi hususları dikkate alınır.
- Bilgi güvenliği olaylarının değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması ve olayların kök nedenine inilmesi ve yazılı hale getirilmesi gerekmektedir.
- 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, internet loglarından faydalanır.
- Olay kanıtlarının korunması yetkili kişilerin dışında erişimi kapatarak veya yedekleme yaparak sağlanır.

- Bu politikaya uygun olarak çalışmayan tüm personel hakkında İnsan Kaynakları Disiplin Prosedürü'nde (TMD_IK_PRD.004) belirtilen Disiplin Yönetmeliği Maddeleri uygulanır.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

ERİŞİM KONTROL POLİTİKASI

Bu politika; yetkili kullanıcı erişimini sağlamak ve yetkisiz erişimi önlemek amacıyla oluşturulmuştur.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş.'nin çalışanlarına sunduğu yazılım ve donanım sistemlerinde, yetkili ve yetkisiz kullanıcı erişimleri, yeni kullanıcıların kayıt başlangıçlarından, bilgi sistemlerine ve hizmetlerine erişim gereksinimi artık kalmamış kullanıcıların son kayıttan çıkışlarına kadar olan basamakları içermektedir.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Erişim Kontrol Politikası doğrultusunda;

- TÜMAD içerisinde giriş çıkışlar kamera sistemi ile kayıt altına alınmalıdır.
- Kullanıcı yetkilendirilmeleri personel bazında yapılmalıdır.
- Kullanıcılar taşınabilir medyaları (cd, usb, vb.) sadece iş amaçlı kullanmalı ve bu medyalar takıldığı zaman antivirüs yazılımı ile taranmalıdır.
- Aktif dizine bağlanan kullanıcı parolaları Şifre Politikasına uygun tanımlanmalıdır.
- Erişim gereksinimi artık kalmamış kullanıcılar için İnsan Kaynakları Prosedürüne göre hareket edilir. Sistemden de bu personelin erişim şifresi silinir.
- Ağ üzerinde aktif dizin kullanıcıları için sürücüler/ortak alanlar oluşturulmalıdır.
- Bu sürücüler üzerindeki birimler ve kullanıcılara göre yetkilendirme yapılmalıdır.
- Yönetim tarafından yetkilendirilen personel haricinde hiç bir personelin dosya silme yetkisi bulunmamalıdır. Silme işlemi sadece ilgili birim amirleri tarafından tanımlanan kişiler tarafından yapılmalıdır.
- TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Z Klasöründeki Entegre Yönetim Sistemleri klasörüne erişimi TÜMAD içi platform üzerinden personellere sunulmaktadır.
- Paylaşımlar Entegre Yönetim Sistemleri yöneticisi tarafından belirlenmektedir.
- TÜMAD Madencilik Sanayi ve Ticaret A.Ş. 'de yayınlanan dokümanlara tüm kullanıcılar QDMS Entegre Yönetim Sistemleri Yazılım programı üzerinden erişebilmekte olup, sadece okuma yetkisine sahiptirler. Entegre Yönetim Sistemleri Bölümü dışındaki kullanıcıların dosya ve/veya form oluşturma, ekleme, değiştirme yetkisi bulunmamaktadır. Bu şekildeki istekleri var ise Entegre Yönetim Sistemi departmanına haber verilmelidir.
- TÜMAD mümkün olduğunca SSL ya da benzeri güvenlik protokollerinin kullanılması benimsenmelidir.

TÜMAD
MADENCİLİK SANAYİ VE TİCARET A.Ş.

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKALARI KABUL ONAYI

TÜMAD Madencilik Sanayi ve Ticaret A.Ş Bilgi Güvenliği Yönetim Sistemi Politikalarında ifade edilen tüm kurallara uymayı, iş bu güvenlik politikalarının ve revizyonlarının Bilgi Güvenliği 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.Bilgi Güvenliği Politikasını okuyunuz.
2.Aşağıdaki belirtilen bölümlere bilgileri doldurup imzalayınız.
3.Bu sayfayı İnsan Kaynakları Müdürlüğü'ne teslim ediniz.

Anlaşma

Bu forma imza atarak Bilgi Güvenliği Politikalarını kabul etmiş oluyorum.

TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Bilgi Güvenliği Politikası kabul onayının bir kopyasını teslim aldım, okudum ve anladım.

Personelin;
İmzası :
T.C. Kimlik No :
Adı ve Soyadı :
Unvanı :
Bölümü :
Tarih :

Bu form TÜMAD Madencilik Sanayi ve Ticaret A.Ş. Bilgi Güvenliği Politikasının okunduğu, anlaşıldığı ve kabul edildiğinin onaylandığı bir dokümandır. TÜMAD'ın yönetim temsilcisi ve Genel Müdür bu politikanın uygulanabilirliğinden sorumludur.