1.AMAÇ

Bu politika HSM Metalurji' de

- Şirketin güvenilirliğini ve temsil ettiği markanın imajını korumak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,
- Şirketin temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak amacıyla bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

2.KAPSAM

Bu politika, HSM Metalurji'nin, Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3.TANIMLAR

Bilgi güvenliği; işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve bilginin geniş çaplı tehditlerden korunmasını sağlar.
Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

1. Gizlilik (Confidentiality)
2. Bütünlük (Integrity)
3. Kullanılabilirlik (Availability)

Bu kavramları biraz daha açacak olursak

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

Bütünlük,
Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması diyebiliriz.

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

4.İLKELER

HSM Metalurji bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:

a)Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
b)Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
c)Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,

d)Bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi İşlem Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalıdır.
e)Şirket içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.

HSM Metalurji 'in tüm çalışanları; bu politikaya, prosedür ve talimatlarına uymakla sorumludur.

a)İş süreçlerinin gereksinimi olarak her türü bilgi, en az kesintiyle kapsam dahilindeki birimler, hizmet verenler ve gereken üçüncü taraflarca erişilebilir olacaktır.
b)Bilgilerin bütünlüğü her durumda korunacaktır.
c)Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınacaktır.
d)Bilgi Güvenliği Yönetim Sisteminin tasarımı, uygulaması ve sürdürülmesi aracılığıyla riskler kabul edilebilir düzeye indirilecektir.
e)Bilgi; bilginin elektronik iletişimi, üçüncü taraflarca paylaşımı, araştırma amaçlı kullanımı, fiziksel ya da elektronik ortamda depolanması gibi kullanım biçimlerinden bağımsız olarak korunacaktır.
f) Bilgi İşlem Sorumlusu bilgi güvenliği uygulanmasından birinci dereceden sorumlu olacaktır ve personelin bu esaslara uygun olarak çalışmasını sağlayacaktır.

4.1. E-Posta Kullanma Kuralları

- HSM Metalurji 'in e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
- Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Kişisel kullanım için internetteki listelere üye olunması durumunda şirkete ait e-posta adresleri kullanılmamalıdır.
- Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.
- Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
- Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir. Çünkü bu mailler virüs içerebilirler.
- Şirket dışından güvenliğinden emin olunmayan bir bilgisayardan web posta sistemi kullanılmamalıdır.
- Çalışanlar, şifrelerin kırıldığını fark ettikleri andan itibaren yetkililerle temasa geçip durumu haber vermekle yükümlüdürler.
- Altı ay süre ile kullanılmayan e-posta kutuları Bilgi İşlem birimi tarafından kaldırılabilir. Kurumdan ayrılan personel kurumsal e-posta sistemini kullanamaz. E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma, işten ayrılma sebepleriyle

kurumdaki değişikliğinin yetkililer tarafından Bilgi İşlem birimine en kısa zamanda bildirilmesi gerekmektedir.

4.2.Şifre Kullanma Kuralları

- Bütün kullanıcıların şifreleri uygun görülen aralıklarda değiştirilmelidir. Tavsiye edilen değiştirme süresi her 6 ayda birdir.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Şifreler başkası ile paylaşılmamalı, kağıtlara ya da elektronik ortamlara yazılmamalıdır.
- E-posta mesajlarında şifre yazılmamalıdır.
- Şifreler, işten uzakta olduğunuz zamanlarda iş arkadaşlarına verilmemelidir.
- Bir kullanıcı adı ve şifresi birden çok bilgisayarda kullanılmamalıdır.

4.3.Antivirüs Politikası

- Bütün bilgisayarda kurumun lisanslı antivirüs yazılımı yüklü olmalıdır ve çalışmasına engel olunmamalıdır.
- Antivirüs yazılımı yüklü olmayan bilgisayar ağa bağlanmamalı ve hemen Bilgi İşlem birimine haber verilmelidir.
- Hiçbir kullanıcı herhangi bir sebepten dolayı antivirüs programını sistemden kaldıramaz ve başka bir antivirüs yazılımını sisteme kuramaz.

4.4.İnternet Kullanım Politikası

- Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek yasaktır.
- İş ile ilgili olmayan (Müzik, video, görsel dosyaları) yüksek hacimli dosyalar göndermek (upload) ve indirmek(download) etmek ve bilgisayarlarda saklamak yasaktır.
- İnternet üzerinden şirket tarafından onaylanmamış yazılımlar indirilemez ve bilgi sistemleri üzerine bu yazılımlar kurulamaz kullanılamaz
- Bilgisayarlar üzerinden genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
- Bilgi İşlem Birimi gerekli durumlarda internet üzerinde kısıtlamalar yapabilir.

4. 5.Genel Kullanım Politikası

- Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3.şahısların bilgilere erişimi engellenmelidir.
- Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.
- Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.
- Şirket bilgilerimiz dışardan üçüncü kişilere iletilmemelidir.
- Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
- Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.

- Şirketin kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD' leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.
- Yetkisi olmayan personelin, şirketteki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
- Personel, kendilerine tahsis edilen ve şirket çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin güvenliği ile sorumludur.
- Bilgi İşlem birimi tarafından yetkili kişiler kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktan bakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
- Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- Kurumda Bilgi İşlem biriminin bilgisi olmadan Ağ sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.
- Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.
- Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
- Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli ve Bilgi İşlem Birimine haber verilmelidir.