1. AMAÇ:

Durmazlar Makina Sanayi ve Ticaret A.Ş.'nin bilgi güvenliğini yönetmekteki amacı; firmanın stratejik hedefleri ve amaçları doğrultusunda, bilgi varlıklarının içeriden ve/veya dışarıdan gelebilecek, kasıtlı veya kazayla oluşabilecek riskleri, gizlilik, bütünlük ve erişilebilirlik yönlerinden değerlendirilerek risk azaltma faaliyetlerinin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesini temin etmektir.

Durmazlar Makina Sanayi ve Ticaret A.Ş. bünyesinde kurulan Bilgi Güvenliği Yönetim Sistemi (BGYS), firma varlıkları ve tedarikçilerden alınan hizmetler dahil, yürütülen tüm faaliyetlerde bilgi güvenliğini sağlamak amacıyla kurulmuştur.

Durmazlar Makina Sanayi ve Ticaret A.Ş. yönetimi "Bilgi Güvenliği Politikası" ve bu politikayı destekleyen alt politikalar ile bilgi güvenliği yönetim sistemine verdiği desteği ifade eder. BGYS politikalarının tüm paydaşların bilgi güvenliği gereksinimini karşılayacak şekilde oluşturulması, sürekli iyileştirilerek yaşatılması ve bu amaçla gerekli kaynakların sağlanması üst yönetimin sorumluluğundadır.

2. KAPSAM ve SORUMLULAR:

Durmazlar Makina Sanayi ve Ticaret A.Ş. bünyesinde kurulmuş ve işletilmekte olan Bilgi Güvenliği Yönetim Sistemi kapsamı dâhilinde aşağıdaki departmanlar ve faaliyetler bulunur.

1. Bilgi Teknolojileri Departmanı
2. İnsan Kaynakları Departmanı
3. Muhasebe ve Finans Departmanı
4. Satış Departmanı
5. Satınalma Departmanı
6. Lojistik / Dış Ticaret Departmanı
7. Arge Departmanı

Durmazlar Makina Sanayi ve Ticaret A.Ş. Bilgi Güvenliği Yönetim Sistemi, aşağıdaki varlık ve teknoloji kategorilerini kapsamaktadır:

- ▪ Veri dosyaları, sözleşmeler, özlük dosyaları, firma imajı, web sitesi vb. den oluşan bilgi varlıkları,
- ▪ Uygulama yazılımları, sistem yazılımları ve hizmetlerinden oluşan yazılım varlıkları,
- ▪ Yönlendirici cihazlar, güvenlik cihazları, sunucular, kullanılan elektronik imza cihazı,

  bilgisayarlar, iletişim donanımı ve veri depolama ortamlarını içeren fiziksel varlıklar,

- ▪ Tüm işlevlerin yerine getirilmesi ile ilgili aydınlatma, iklimlendirme, kablolama gibi unsurlardan

  oluşan hizmet varlıkları,

- ▪ Kapsamdaki faaliyetlerin yürütülmesini sağlayan insan kaynakları varlıkları,
- ▪ Hizmet alınan sözleşmeli veya sözleşmesiz tedarikçiler,
- ▪ Müşteriler ve bayiler
- ▪ BGYS dokümanları ve kayıtları.

3. İLGİLİ DÖKÜMANLAR:

   Tüm BGYS Dokümantasyonu

4. UYGULAMA :

4.1. Tanımlar

1. 4.1.1. Bilgi : Bilgi, kurum için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır.
2. 4.1.2. BilgiGüvenliği : Firma bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik özelliklerinin korunmasıdır. Bilgi güvenliği, iş sürekliliğini sağlamak, kayıpları en aza indirmek için varlıkları tehlike ve tehdit alanlarından korur.

   Bilgi güvenliği, aşağıdaki bilgi niteliklerinin korunmasını hedefler:

   Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etmek. Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu, yetkisiz değiştirmelerden

   korunmasını ve değiştirildiğinde farkına varılmasını temin etmek.

   Erişilebilirlik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerini garanti etmek.

4.1.3. Bilgi Güvenliği Politikası :

HER NEVİ MAKİNE VE RAYLI SİSTEMLER ÜRETİMİ, SATIŞI VE PAZARLAMASI İÇİN YAPILAN İTHALAT, İHRACAT, TRANSİT, GÜMRÜKLEME, DIŞ TİCARET İŞLEMLERİ VE BU İŞLEMLERE İLİŞKİN LOJİSTİK, DEPOLAMA, FİNANS, ARGE, MUHASEBE VE BİLGİ İŞLEM FAALİYETLERİNİN GERÇEKLEŞTİRİLMESİNDE;

İNSAN, ALT YAPI, YAZILIM, DONANIM, MÜŞTERİ BİLGİLERİ, KURULUŞ BİLGİLERİ, ÜÇÜNCÜ ŞAHISLARA AİT BİLGİLER VE FİNANSAL KAYNAKLAR İÇERİSİNDE BİLGİ GÜVENLİĞİ YÖNETİMİNİN SAĞLANDIĞINI GÖSTERMEK, RİSK YÖNETİMİNİ GÜVENCE ALTINA ALMAK, BİLGİ GÜVENLİĞİ YÖNETİMİ SÜREÇ PERFORMANSINI ÖLÇMEK VE BİLGİ GÜVENLİĞİ İLE İLGİLİ KONULARDA ÜÇÜNCÜ TARAFLARLA OLAN İLİŞKİLERİN DÜZENLENMESİNİ SAĞLAMAK.

BU DOĞRULTUDA;

- • İÇERİDEN VEYA DIŞARIDAN, BİLEREK YA DA BİLMEYEREK MEYDANA GELEBİLECEK HER

  TÜRLÜ TEHDİDE KARŞI KURULUŞUMUZUN BİLGİ VARLIKLARINI KORUMAK, BİLGİYE ERİŞEBİLİRLİĞİ İŞ PROSESLERİYLE GEREKTİĞİ ŞEKİLDE SAĞLAMAK, YASAL MEVZUAT GEREKSİNİMLERİNİ KARŞILAMAK,

- • YÜRÜTÜLEN TÜM FAALİYETLERDE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN ÜÇ TEMEL ÖĞESİNİN SÜREKLİLİĞİNİ SAĞLAMAK.
- • GİZLİLİK: ÖNEM TAŞIYAN BİLGİLERE YETKİSİZ ERİŞİMLERİN ÖNLENMESİ,
- • BÜTÜNLÜK: BİLGİNİN DOĞRULUK VE BÜTÜNLÜĞÜNÜN SAĞLANDIĞININ GÖSTERİLMESİ,
- • ERİŞEBİLİRLİK: YETKİSİ OLANLARIN GEREKTİĞİ HALLERDE BİLGİYE ULAŞILABİLİRLİĞİNİN

  GÖSTERİLMESİ,

- • SADECE ELEKTRONİK ORTAM DA TUTULAN VERİLERİN DEĞİL; YAZILI, BASILI, SÖZLÜ VE

  BENZERİ ORTAM DA BULUNAN TÜM VERİLERİN GÜVENLİĞİNİ KORUMAK.

- • BİLGİ GÜVENLİĞİ YÖNETİMİ EĞİTİMLERİNİ TÜM PERSONELE VEREREK BİLİNÇLENDİRMEYİ SAĞLAMAK.
- • BİLGİ GÜVENLİĞİNDEKİ GERÇEKTE VAR OLAN VEYA ŞÜPHE UYANDIRAN TÜM AÇIKLARIN, BGYS EKİBİNE RAPOR ETMEK VE BGYS EKİBİ TARAFINDAN SORUŞTURULMASINI SAĞLAMAK.
- • İŞ SÜREKLİLİK PLANLARI HAZIRLAMAK,SÜREKLİ İYİLEŞTİRMEK, SÜRDÜRMEK VE TEST ETMEK.
- • BİLGİ GÜVENLİĞİ KONUSUNDA PERİYODİK OLARAK DEĞERLENDİRMELER YAPARAK MEVCUT RİSKLERİ TESPİT ETMEK. DEĞERLENDİRMELER SONUCUNDA, AKSİYON PLANLARINI GÖZDEN GEÇİRMEK VE TAKİBİNİ YAPMAK.
- • SÖZLEŞMELERDEN DOĞABİLECEK HER TÜRLÜ ANLAŞMAZLIK VE ÇIKAR ÇATIŞMASINI ENGELLEMEK.
- • BİLGİYE ERİŞEBİLİRLİK VE BİLGİ SİSTEMLERİ İÇİN İŞ GEREKSİNİMLERİNİ KARŞILAMAKTIR.

Bilgi güvenliği politikası dokümanı, yukarıdaki gereksinimleri sağlayabilmek için oluşturulmuş denetimlerin uygulanması sırasında kullanılacak en üst seviyedeki prensiplerin belirtildiği dokümandır.

Daha alt düzeyde; bilgi güvenliği politikası, bilgi güvenliği kontrollerini zorunlu tutan konuya özel politikalarla desteklenmiştir. Konuya özel politikalar kuruluşun içinde belirli hedef gruplarının ihtiyaçlarını karşılamak ya da belirli konuları kapsayacak şekilde yapılandırılmıştır:

4. 4.1.4. BGYS : Bilgi Güvenliği Yönetim Sistemi
5. 4.1.5. BGYS Komitesi : Kurum içerisinde ilgili tüm birimlerden katılımcıların bulunduğu üst yönetimin de temsil edildiği bilgi güvenliği yönetim sisteminde stratejik kararları vererek, Yönetim Gözden Geçirme faaliyetini yürüten kuruldur.

4.2. Bilgi Güvenliği Yönetiminde Roller ve Sorumluluklar 4.2.1. Üst Yönetimin Desteği ve Sorumluluğu

Üst yönetim;

1. a) Firmanın stratejik hedefleri doğrultusunda, Bilgi Güvenliği Politikasını ve Bilgi Güvenliği Yönetim sistemini oluşturmaktan ve hedeflerini belirlemekten,
2. b) Yönetim Gözden Geçirmesi faaliyetine katılmaktan,
3. c) BGYS altyapısı ihtiyaçlarına, işleyişini devam ettirilmesine ve sürekli iyileştirme faaliyetlerine destek vermekten,
4. d) BGYS yaşatılması ve geliştirilmesi için kaynak ayırmaktan,
5. e) BGYS komitesinin oluşturulmasından, komitenin rol ve sorumluluklarının belirlenmesinden, işleyişinin takip edilmesinden ve sistemin geliştirilmesinden sorumludur.

4.2.2. BGYS Yönetim Temsilcisi ve BGYS Komitesinin Sorumluluğu BGYS Yönetim Temsilcisi ve BGYS Komitesi;

1. a) Bilgi Güvenliği Politikasını ve alt politikaları yönetmekten,
2. b) Risk Değerlendirme faaliyetlerini planlamaktan ve uygulamaktan,
3. c) BGYS farkındalığını arttırıcı faaliyetleri planlamak ve uygulamaktan,
4. d) Üst yönetimden destek talep etmekten,
5. e) İhlal olaylarını incelemekten ve kök nedenlerin bulunmasından, üst yönetime raporlamadan, risk değerlendirmelerinin yapılmasından,
6. f) Yönetim Gözden Geçirmesi faaliyetini yürütmekten,
7. g) İç denetimleri planlamak ve uygulamaktan,
8. h) BGYS performansını üst yönetime raporlamaktan,
9. i) BGYS altyapısını desteklemek, işleyişini devam ettirmek ve sürekli iyileştirme faaliyetleri ile sistemi devamlı suretle yaşatmak ve geliştirmekten,
10. j) BGYS politika ve prosedürlerini yayınlamaktan ve tüm çalışanlara bildirmekten, sorumludur.

4.2.3. Birim Yöneticilerinin Sorumluluğu

Birim yöneticileri, Bilgi Güvenliği Politikasını uygulamak ve çalışanlarının esaslara bağlılıklarını sağlamaktan sorumludur.

4.2.4. Çalışanların Sorumluluğu

Her çalışan,

1. a) Bilgi Güvenliği Politikası ve alt politikalarını bilmekten; bu kural ve esaslara uygun davranmaktan, bunların gereğini bilgi güvenliği prosedürlerini ve formlarını kullanarak gerçekleştirmekten,
2. b) Firma bünyesindeki bilgi varlıklarını, “PL.BG.02 - Varlıkların Kullanımı Poitikası” na uygun olarak kullanmaktan,

c) Müşteri ve tedarikçi ilişkileri dahil olmak üzere “PL.BG.03 – Bilgi Güvenliği İhlal Olayı Yönetimi Politikası”na uygun şekilde güvenlik ihlallerini bildirmekten,

4. d) Bilgi Güvenliği Yönetim Sisteminin geliştirilmesi için uygun gördüğü önerileri BGYS komitesi üyelerine iletmekten ve “FR.BG.06 – Düzeltici ve Önleyici Faaliyet Talep Formu”nu işletmekten,
5. e) “PL.BG.04 – Yasal Gereksinimlere Uyum Politikası “ gereğince, T.C. yasaları, yönetmelikler, genelgeler ve sözleşmeler ile uyumlu çalışmaktan,
6. f) Bilgi güvenliği ile ilgili eğitimlere, tatbikatlara katılmaktan, acil durumlarda kiminle, nasıl irtibata geçilmesi gerektiğini bilmekten sorumludur.

4.2.5. Tedarikçilerin Sorumluluğu Bilgi varlıklarına erişen her tedarikçi,

1. a) Kurumun Bilgi Güvenliği Politikasını okumaktan,
2. b) Bilgi güvenliği anlaşması imzalamaktan,
3. c) Gereken bilgi varlıklarına, kaynaklara ve alanlara kurumun Bilgi Güvenliği Politikası, Erişim Politikası ve Fiziksel Güvenlik Politikası kuralları çerçevesinde erişmekten ve gerekli uyumu göstermekten,
4. d) İhlal olayları durumunda istenen bilgileri sağlamaktan ve işbirliği yapmaktan, sorumludur.

4.3. Bilgi Güvenliği Politikasının Gözden Geçirilmesi

Bilgi Güvenliği Politikası ve alt politikaları organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından değerlendirilir. Bu esaslar düzenli olarak, yılda en az bir (1) kez Yönetim Gözden Geçirme (YGG) toplantısında gözden geçirilir.