Bilgi Güvenliği Politikası / *Information Security Policy*

1. Bilgi Güvenliği Yönetim Sistemi / *Information Security Management System*

- HAVELSAN Bilgi Güvenliği Yönetim Sistemi, Bilgi Güvenliği Yönetim Sistemi Prosedürü ve bağlı diğer prosedür ve talimatlarla tanımlanmış esaslar ve sorumluluklar doğrultusunda gerçekleştirilir ve sürekli iyileştirilir.
- Bilgi Güvenliği Yönetim Sisteminin oluşturulmasını, sürdürülmesini ve etkinliğini temin etmek üzere doğrudan Genel Müdür'e bağlı olarak görev alan ve BGYS ile ilgili sorunların çözümü için Şirket içinde gerekli bağımsızlığa ve yetkiye sahip olan Yönetim Temsilcisi, Operasyonlar Genel Müdür Yardımcısı olarak belirlenmiştir. Yönetim Temsilcisi en üst seviyede BGYS uygulamalarına liderlik ve bağlılık gösterir.
- Kurumsal Bilişim Hizmetleri Müdürlüğü bilgi güvenliği konusunda bilgi seviyesini ve kurumsal yetkinliği geliştirmek ve güncel tutmak, bilgi güvenliğine yönelik saldırı ve korunmasızlıklara ait gelişmelerden erkenden haberdar olup, önlem almak, yeni bilgi güvenliği teknolojileri ve ürünleri ile ilgili gelişmeleri takip etmek ve bilgi güvenliği olaylarının üstesinden gelmek için uygun irtibat noktaları geliştirmek amacıyla, dernek, şirket ve kurumlardan oluşan özel ilgi grupları ile iletişim içinde bulunur, bu kapsamdaki etkinliklere katılır.

2. Varlık Yönetimi / *Asset Management*

- Şirket için değerli elektronik ve basılı ortamdaki her türlü bilgi ile bilgi işleme aracı / kabiliyeti, HAVELSAN bilgi varlıklarını oluşturur.
- Şirket paydaşları (sermayedar, müşteriler, hükümetler, iş ortakları, alt yükleniciler, vb.) tarafından, sözleşmeler, gizlilik anlaşmaları, yasal mevzuat vs. ile tanımlanmış esaslar dâhilinde HAVELSAN kullanımına verilmiş varlıklar da bilgi varlıkları kapsamında değerlendirilir.
- Bilgi varlıkları, değer farkı gözetmeksizin, kasten veya kazara ortaya çıkabilecek iç ve dış tehdit ve korunmasızlıklara karşı korunur.
- Bu kapsamda tüm birimler ve çalışanlar bilgi varlıklarını, kasten veya kazara, yetkisiz erişime, değiştirilmeye, kopya edilmeye, tahrif ve yok edilmeye veya ifşa edilmeye karşı korumakla sorumludur.
- Sabit disk, harici disk, USB bellek, flaş bellek kartları, disket, CD, DVD ve BD gibi taşınabilir her türlü kişisel veya özel mülkiyet depolama ortamının şirkete girişi ve kullanımı yasaktır.
- Şirkete ait taşınabilir bilgi işleme ortam ve cihazları, yetkisiz erişime neden olacak şekilde gözetimsiz bırakılmaz. Şirket gizli bilgisi taşınabilir bilgi işleme cihazlarında şifresiz olarak saklanamaz. Şirket tarafından onaylanmış şifreleme yöntemleriyle korunmalıdır.
- Şirket tarafından onaylanmış şifreleme yöntemleri ve iletim metotları kullanılmadan Şirket bilgisi, taşınabilir bilgi işleme cihazlarından veya bu cihazlara kablosuz olarak aktarılamaz. Ayrıca bilgi, zararlı yazılımlara karşı taramadan geçirilmeden Şirket ağına aktarılamaz.
- Şirket bilgi varlıkları ve bilgi işleme imkânları kapsamına giren evrak, yazılım ve donanımın şirket dışına çıkışı Evrak ve Malzeme Güvenliği Prosedürüne göre gerçekleştirilir.

- Bilgi varlıkları, şirkete olan önemlerini ve hassasiyetlerini gösterecek şekilde, gizlilik derecesine göre sınıflandırılır ve etiketlenir.
- Bilgi varlıkları, belirtilen gizlilik derecesine uygun olacak şekilde ele alınır, kullanılır, işlenir ve saklanır.
- Ev bilgisayarları, dizüstü, tablet bilgisayarlar ve avuç içi cihazlar gibi her türlü kişisel veya özel mülkiyet bilgi işlem imkânının şirkete girişi ve kullanımı yasaktır.
- Kişisel veya özel mülkiyet cep telefonlarının şirket içinde görüntü alımı ve şirkete ait elektronik bilgi varlıklarının yetkisiz erişime olanak sağlayacak şekilde aktarımı için kullanılması yasaktır.
- İnternet dâhil şirkete ait ağlar, şirket e-posta hesapları, telefon ve bilgisayarlar gibi şirkete ait bilgi işleme imkânları sadece iş amaçlı kullanım içindir. Bu kaynakların kişisel amaçlı kullanımı sınırlandırılmıştır. Asla kişisel kazanç maksatlı, iş ahlâkına aykırı, zararlı, yasadışı amaçlara yönelik veya kamuoyunda şirket adına mahcubiyet oluşturacak şekilde kullanılamazlar. Her durumda bu kaynakların kullanımının, yasa ve yönetmeliklere aykırı olması, çalışanların veya diğer kişi ve kurumların haklarına yönelik olumsuz tutum ve davranış içermesi, iş ve kaynakların etkinlik ve verimliliğini olumsuz yönde etkilemesi kabul edilemez.
- Benzer şekilde Şirkete ait yazılımlar yasa dışı, Şirket politikalarına aykırı veya Şirket çıkarlarına ters düşecek şekilde kullanılamaz. Şirkete ait yazılımların izinsiz çoğaltılması yasaktır.
- Şirketin İnternet kaynakları onaylanmamış, ücretsiz veya ticari hiçbir yazılımın dağıtılması, indirilmesi veya yüklenmesi için kullanılmaz.
- Kullanıcılar sadece Şirketin yetkili birimlerince onaylanmış e-posta yazılımlarını ve yapılandırmalarını kullanabilirler.
- Bilgi varlıklarına erişim, “Bilmesi Gereken” ve “En Az Haklar” ilkesine göre verilen yetkiler çerçevesinde sağlanır.
- Bilgi varlıkları, tanımlı varlık sahibi sorumluluğundadır. Bilgi varlıklarının geçici devri, bilgi güvenliği kapsamındaki sorumluluğun devri anlamına gelmez.
- Bilgi varlıkları, yetkisiz olarak üçüncü taraflara ifşa edilemez, aktarılamaz ve kullandırılamaz.
- Çalışanlar, işleri ile ilgili araştırma ve sorun çözme faaliyetlerinde, "Bilmesi Gereken" kapsamına girmeyen şirket içi / dışı kişi ve kuruluşlardan bilgi ve yardım alırken veya iletişim halindeyken, müşteri, HAVELSAN, proje, tüm proje unsurları ve ekibi ile ilgili bilgiler ile üçüncü taraflara ait (Bilgi Gizliliği Anlaşması ile korunan) bilgileri ifşa edemez. Bu tür araştırma / iletişim faaliyetlerinde, bilgilerin gizliliğini koruyacak şekilde, bilgi güvenliği sorumluları denetiminde hareket edilmelidir.
- Her türlü sosyal medya ortamında, HAVELSAN'ın kurumsal itibarını, çalışanlarının onurunu ve mahremiyetini etkileyecek görüş, fikir, beyan ve ileti paylaşılamaz.
- Şirket, bilgi işleme imkânlarını ve bu imkânların kullanımına yönelik faaliyetleri, izleme, kaydetme ve belirli aralıklarla denetleme hakkını saklı tutmaktadır.
- Bilgi varlıklarının uygun görülen kullanımı ile ilgili diğer esaslar Kabul Edilebilir Kullanım Talimatında tanımlanmaktadır.

3. İnsan Kaynakları Güvenliği / *Human Resources Security*

- Bilgi güvenliği farkındalığı, tüm çalışanlar ve paydaşlar için oluşturulur; bu farkındalığın sürdürülmesine yönelik, düzenli eğitim, idman ve bilgilendirme çalışmaları yapılır.

- İş kartvizitlerinde ve kurumsal e-postalarda verilen iletişim bilgilerinde, yalnızca şirket tarafından tahsis edilen iletişim araçlarına ilişkin bilgiler verilebilir; özel cep telefonu veya ev telefon numarası, özel e-posta hesabı, ev adresi gibi iletişim bilgilerine yer verilmez.
- İstihdam öncesinde, çalışma süresince ve istihdam sonrasında; bilgi güvenliğine ilişkin çalışanları yasal yönden bağlayıcı ve bilgilendirici önlemler alınır.
- İşe alım sırasında, başvuruda sunulan referans kişileri, özgeçmiş ve mülakatta verilen bilgileri, yazılı veya sözlü iddia edilen akademik ve profesyonel vasıfları, kimlik bilgileri ve adli sicil kayıtlarını doğrulatan denetimler yapılır.
- Telefon ve e-posta gibi araçlar ile iletişimde karşı tarafın kimliğinden emin olunmadığı durumlarda iletişimi sonlandırıp kimlik doğrulaması tam olarak yapılmadan hareket edilmez.
- İnsan kaynakları güvenliğine yönelik diğer bilgi güvenliği esasları, İnsan Kaynakları Yönetimi Sürecinde Personel İşlemleri Prosedürü ile Personel Planlama ve Seçme Esasları Prosedüründe tanımlanmaktadır.

4. Fiziksel ve Çevresel Güvenlik / *Physical and Environmental Security*

- Birimlerin yürüttüğü projeler için bir birinden mantıksal veya fiziksel olarak yalıtılmış güvenlik seviyesine uygun ortamlar oluşturulur.
- Çalışma masası çevresinde ve çalışma bilgisayarlarında bulunan hassas bilgi malzemelerini geçici terk ederken ve normal çalışma saatleri dışında uzun süreli sahipsiz bırakırken, yetkisiz erişim, kaybolma ve hasar görme riskini azaltmaya yönelik “Temiz Masaüstü” ve “Temiz Ekran” ilkesi tüm çalışanlar tarafından uygulanır.
- Yükleme/boşaltma/malzeme teslimat alanları gibi 3.taraflarla etkileşimin yoğun olduğu bölgelerde bilgi işleme olanaklarına 3.tarafların yetkisiz erişimine zemin oluşturacak hususlara karşı özellikle dikkat edilir. Temiz Masa/Temiz Ekran ilkesine kesinlikle uyulur. Bilgi işleme olanakları geçici kısa süre ayrılıklarda bile kilitlenir ya da korumaya alınır.
- Şirkete iş takibi ya da toplantı amacıyla gelen ziyaretçilerin cep telefonu ve diğer mobil cihazlarının şirket içine alınmasına izin verilmemektedir. Ziyaretçi telefonları nizamiyede özel mülkiyet için ayrılmış dolaplarda muhafaza edilmekte ve şirkete alınmamaktadır.
- Fiziksel ve çevresel güvenlik ile ilgili diğer bilgi güvenliği esasları Bilgi Güvenliği Yönetim Sistemi Prosedüründe ve Fiziki Güvenlik Prosedüründe tanımlanmaktadır.

5. Haberleşme ve İşletim Yönetimi / *Communications and Operations Management*

- Bilgisayar virüsleri, solucanları, truva atları, casus yazılımlar, arka kapılar, klavye dinleme sistemleri ve mesaj sağanakları (spam) gibi kötücül yazılımların (malware); mobil veya yerleşik bilgi işleme imkânlarına bulaşması, yayılması ve zarar vermesi, kendiliğinden devreye giren ve sık sık güncellenen güçlü kötücül yazılım önleyici yazılımlar ile engellenir.
- Kötücül yazılımları, şirket bilgi işleme imkânlarına yerleştirmek ve yaymak yasaktır.
- Bilgilerin bütünlüğü ve kullanılabilirliğinin temin edilmesi için sıkı bir şekilde takip edilen, etkin bir yedekleme politikası yürütülür.
- Kullanıcıların bilgi işleme imkânlarını kullanımının, başarılı/başarısız kimlik denetimi ve yetkilendirmelerinin, sistem program hatalarının ve bilgi sistemlerinin

yönetiminden sorumlu sistem yöneticilerinin kullandığı uygulamaların günlükleri tutulur ve koruma altında saklanır.

- Şirketin farklı yerleşkeleri ve sahaları arasındaki güvenli veri iletişimini sağlamak amacıyla intranet ağında ticari algoritmaya sahip kripto cihazları kullanılır.
- Bilgi varlıklarına yönelik sorumluluklar “Görevler Ayrılığı” ilkesine göre mümkün olduğunca tek bir kişide toplanmayacak şekilde yönetilir.
- Hassas veya kişisel bilgilerin tutulduğu ortamlar elden çıkarılırken güvenli bir şekilde silinir. Kâğıt ortamındaki belgeler kâğıt kırpma makinaları kullanarak ve diğer manyetik ve optik ortamlar ilgili birimden destek alınarak güçlü yöntemlerle silinip/yok edilmeden elden çıkarılamaz veya devredilemez.
- Haberleşme ve işletim kapsamında alınması gereken bilgi güvenliği önlemleri "Yanıltıcı Güvenlik Algısına" neden olmayacak şekilde belirlenir.

6. Erişim Kontrolü / *Access Control*

- Bilgi işleme imkânlarının kullanımı, kullanıcı tabanında erişim kontrolü işleyişi ile mümkündür.
- Kullanıcı tescili ve kayıt değişimi şirket prosedürleri doğrultusunda yalnızca yetkili kişiler tarafından yapılır.
- Bilgi güvenliğine yönelik beyan edilsin ya da edilmesin hiçbir erişim kontrolü kullanıcılar tarafından kaldırılamaz veya hizmet dışı bırakılamaz.
- Erişim kontrolü için başta kullanıcı adı ve parolası olmak üzere akıllı kart ve biyometrik kimlik denetimi gibi gelişmiş yöntemler kullanılır.
- Erişim kontrolünün yetkilendirme safhasında Bilgi Varlıklarına “Bilmesi Gereken” ve “En Az Haklar” ilkesine göre erişim izni verilir.
- Kullanıcılar kimlik denetiminde kullanılan bilgilerini (Kullanıcı Adı ve Parola) ve araçlarını aile üyeleri, yardım masası, her düzeyde yönetici, bilgi güvenliği organizasyonu unsurları, harici ve dâhili tetkikçiler dâhil hiç kimseyle paylaşamaz.
- Kimlik denetimi bilgileri kâğıt, not defteri veya ajanda sayfası, yapışkan not, bilgisayar kasası ve ekranı ve masa üzerine yazılarak basılı şekilde veya elektronik olarak bilgisayar ve ağ ortamında hatırlamak maksadıyla tutulmaz.
- Bilgisayarlara parola girişleri kimsenin göremeyeceği şekilde yapılır.
- Kullanıcılar bir başkasına ait kimlik denetimi bilgi ve araçlarını kullanamaz.
- Kullanıcı adı ve parola ile kimlik denetiminde; ilk atanan boş olmayan parola hemen değiştirilerek, kırılması ve tahmin edilmesi zor ancak hatırlaması kolay yeterince uzun ve güçlü kişisel parolalar tanımlanır. Belli sürelerde eski parolalardan farklı olacak şekilde parola değişikliği mecbur tutulur.
- Bilgi varlıklarına kontrollü erişimi sağlayan yetkiler kişisel değil; tanımlı roller ve/veya kullanıcı grupları tabanında atanır.
- Bu atamanın dışında ihtiyacı ortaya çıkan erişim ayrıcalıkları çok zorunlu hallerde, kısıtlı kapsamda ve kısa süreliğine tanımlanır ve ihtiyaç karşılanır karşılanmaz geri alınır ve ayrıcalık hareketleri kayıt altında tutulur.
- Görev değişiklikleri ve ayrılmalarda kullanıcılara ait tüm yetki ve ayrıcalıklar kaldırılır.
- Bilgi işlem imkânlarına yönetim amaçlı erişim hakkı, görev sorumlulukları dâhilinde

hareket etmek kaydıyla sadece yetkili sistem yöneticilerine verilir.

- Şirketin harici ve dâhili ağları mantıksal ve fiziksel şekilde bilgi sistemlerinin, kullanıcılarının ve hizmetlerinin gruplandığı alt kısımlara ayrılır.
- Enerji tasarrufu ve bilgi güvenliği kapsamında kişisel bilgisayarlar mesai bitiminde veya uzun süreli ayrılıklarda tamamen kapatılır.

7. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı / *Information Systems Acquisition, Development and Maintenance*

- Edinilen bilgi sistemleri kapsamında var olan yazılımlara ait güncellemeler ve yamalar güvenlik zayıflıklarını azaltmak amacıyla kontrollü bir şekilde tatbik edilir.
- Giriş/çıkış verilerin doğrulamasının yapılması, iç veri işlemenin hataya sebep olmayacak şekilde gerçekleştirilmesi ve ileti bütünlüğün sağlanması gibi yöntemlerle güvenli yazılım geliştirme yöntemi takip edilir.
- Bilgi güvenliği durum tespiti yapmak ve gerekli önlemleri almak için sızma testleri düzenli olarak yapılır. Tespit edilen açıklıklar ve riskler için düzeltici ve önleyici faaliyetler gerçekleştirilir.
- Kullanıcılara tahsis edilen bilgisayarlarda ön kurulumlu bir şekilde var olan lisanslı yazılımlar bilgisayarın kullanım amacına göre oluşturulmuş disk yansılarına (imaj) uygun olarak yapılandırılır.
- Ön kurulumda var olan yazılımlar dışında kurulumu talep edilen yazılımların lisanslı ve bilgi güvenliği açısından risk doğurmayacak yazılım olması kontrolleri yapılır.

8. Bilgi Güvenliği Olay Yönetimi / *Information Security Incident Management*

- Kullanıcılar sadece tanınan yetkilerini kullanamadığında değil tanınmamış/talep edilmemiş yetkilerini kullanabildiklerini fark eder etmez, bilgi güvenliği sorumluları ve yetkili sistem yöneticilerine haber vermek zorundadır.
- Bilgi güvenliğini sekteye uğratacak kötü niyetli olaylar, erişim ihlâlleri, çevresel hasarlar, bilgi varlıklarının uygunsuz kullanım örnekleri, bilgi varlıklarına yönelik hırsızlık ve kayıp olayları, elektronik iletişim ortamında olağan dışı tarzda muhatap olunma ve diğer sosyal mühendislik olayları gibi olaylardır. Bu ve benzeri şüpheli durumlar ile karşılaşılır karşılaşılmaz, Bilgi Güvenliği Olay İnceleme ve Değerlendirme Prosedüründe tarif edildiği şekilde ilgili birim ve sorumlulara derhal haber verilir.
- Bilgi güvenliği ihlâl olayı yönetimi ile ilgili diğer esaslar Bilgi Güvenliği Olay İnceleme ve Değerlendirme Prosedüründe tanımlanır.

9. İş Sürekliliği Yönetimi / *Business Continuity Management*

- Şirketin hayati iş süreçlerinin devamlılığını sağlamak, sağlanamadığı şartlarda ön görülen kesinti süreleri içinde yeniden çalışır hale getirmek için bilgi güvenliğinin de dikkate alındığı şirket iş sürekliliği yönetim sistemine göre hareket edilir

10. Uyum / *Compliance*

- Şirket bilgi varlıkları yasalarla belirlenmiş mevzuata, yapılan iş ve ticaret sözleşmelerindeki hükümlere aykırı olacak şekilde kullanılamaz.
- Telif ve fikri mülkiyet hakları kapsamında bilgi işleme imkânlarında, şirketin kendi geliştirdiği yazılımlar ve lisanslanmış veya geliştiricisi tarafından doğrudan şirkete tahsis edilmiş yazılımlar kullanılır.

- Bilgi işleme imkânlarının kötüye kullanımını saptamak ve önlemek için saldırı tespit ve önleme, güvenlik duvarı, içerik denetleme ve diğer izleme araçları kullanılır.
- Hassas bilgilerin yetkisiz kişilere ifşası Bilgi Değişimi ve Gizlilik Anlaşmaları ile önlenir.
- Yapılan iş ve ticaret sözleşmelerinde bilgi güvenliği açısından edinilen bilgilerin gizliliği ve ilgili tarafların bu kapsamdaki sorumlulukları bilgi güvenliğine yönelik maddeler ile güvence altına alınır. Bilgi değişimi gerektiren çalışmalarda ve alt yüklenicinin şirkette çalışması sırasında bilgiye erişmesi gereken durumlarda, uyulacak güvenlik ile ilgili kurallar, bu sözleşmeler içerisinde yönetilmektedir.
- Bu sözleşmeler imzalanmadan ve ilgili tarafa güvenlik bilgilendirmesi yapılmadan bilgi paylaşımı mümkün değildir. Firmalara verilmesi gerekli olan bilgilerde konu ile ilgili olmayan ve firmayı ilgilendirmeyen bilgiler ve şirkete ait bilgiler çıkartılarak verilir.
- Bilgi Güvenliği Politikası ile destekleyici diğer belgelerde yer alan ilkeler, gerektiğinde sözleşmeler, yasa hükümleri ve üst yönetim kararları doğrultusunda, Kalite Sistem Müdürlüğü eşgüdümü ile dış paydaşlarla paylaşılabilir.
- Kişisel Verilerin Korunması Kanununa (KVKK) uyum kapsamında kişisel veri işleme ile ilgili tüm hususlar HAVELSAN Hava Elektronik Sanayi Ve Ticaret A.Ş. Kişisel Verilerin Korunması ve İşlenmesi Politikasında (HVL-KEK / EK-E) verilmektedir.
- Bilgi Güvenliği Politikasına ve bu politikayı destekleyen diğer politika, prosedür ve talimatlara ve iş ve ticaret sözleşmeleri ve yasal mevzuatın getirdiği bilgi güvenliği hükümlerine uyulmaması halinde, HAVELSAN Disiplin Prosedürü hükümleri uygulanır.