YILDIZ HOLDİNG BİLGİ GÜVENLİĞİ POLİTİKASI

Amaç ve Kapsam

Bu politika Yıldız Holding ve Grup şirketleri çalışanlarının uyması gereken bilgi güvenliği kurallarını açıklar.

Bilgi güvenliği nedir?

Şirket için değeri olan tüm dijital yada basılı bilgi, "bilgi varlığı" olarak adlandırılır. Bilgi Güvenliği, bu bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin yeterli seviyede korunabilmesi için uyulması gereken kuralları ve sağlanması gereken uygun koşulları tanımlar.

Bilgi güvenliği politikası neden gereklidir?

Bilgi güvenliği politikaları, bütün çalışanlarca izlenebilecek en iyi bilgi güvenliği uygulamaları çerçevesini oluşturmaya ve ilgili riskleri en aza indirecek gündelik uygulamaları ortaya koymaya yöneliktir. Bilgi güvenliği politikaları ayrıca Şirketin tabi olduğu standartlar ve yasal gereksinimlere uyumlu olabilmesi için gereken hedef kontrol yapısının ortaya konmasında yardımcı olur.

Bilgi güvenliği politikasının temel amaçları

- Bireyi ve bilgiyi korumak,
- Şirketin bilgi güvenliğine yaklaşımını aktarmak,
- Kullanıcı, sistem yöneticileri, yönetim ve güvenlik personelinden beklenen sorumlulukları belirlemek,
- Bilgi Güvenliği personelinin yetkilerini belirlemek,
- İhlallerin sonuçlarını aktarmak,
- Riskin azaltılmasına yardımcı olmak,
- Yasal gereksinimlerle uyumluluğun takibine yardımcı olmaktır.

Tüm Şirket çalışanlarının bilgi güvenliği politikasına uygun şekilde kendi iş süreçlerini yapılandırmaları, ilgili önlem ve tedbirleri almaları gerekmektedir. Bu nedenle bilgi varlığının iş ve teknik sahipleri, sorumlusu oldukları bilgi varlıklarında ve temel iş süreçlerinde politikalarda yazan kuralların uygulanmasından sorumludur.

Bilgi Güvenliği Kurulu

Bilgi Güvenliği Kurulu("BGK" olarak ifade edilecektir), Yıldız Holding ve Grup şirketlerinin bilgi güvenliğinin sağlanması için hedef ve stratejilerinin oluşturulması, konu ile ilgili süreç, standart ve kontrol gereksinimlerinin belirlenmesi, geliştirilmesi ve uygulanması, politikaların ve talimatların yayınlanması ve gerçekleşebilecek bilgi güvenliği olaylarının yönetilmesi konularında yetkilidir.

Yetki ve İhlaller

Belirlenmiş bu usul ve yöntemlerin ihlali halinde "Bilgi Güvenlik Kurulu" ihlali değerlendirir. Bilgi Güvenlik Kurulu bu değerlendirmesini yaparken Yıldız Holding çalışanları ile ilgili konuları Holding ve/veya ilgili Şirket'in İnsan Kaynakları yetkilileriyle istişare eder. Gerekli gördüğü durumlarda kişi ve/veya olayları, Etik Kurulu veya Onur Kurulu'na sevk eder.

Son Kullanıcı Güvenliği

Kapsam: Yıldız Holding ve Grup şirketleri("Şirket" olarak ifade edilecektir) çalışanlarınca kullanılan PC/Dizüstü bilgisayarların ve Şirket ağlarına dahil olmuş mobil cihazların taşıdığı, işlediği ve ilettiği bilginin güvenliği konularını içerir.

1. **PC/Dizüstü Bilgisayarlar:**

1.1 Çalışanlar, Bilgi Sistemleri Genel Müdürlüğü("BSGM" olarak ifade edilecektir) tarafından onaylanmış ve yayınlanmış standart donanımları (PC/Dizüstü bilgisayarlar vb.) ve bu donanımlar üzerinde yine BSGM tarafından onaylanmış standart yazılımları kullanabilir.

1.2 Kullanıcılara sağlanmış bilgisayarlar sadece iş amaçlı kullanılabilir. Sağlanmış donanım ve yazılımda BSGM onayı alınmadan değişiklik yapmak, amacından farklı kullanmak yasaktır.

1.3 Çalışanlara Şirket tarafından tedarik edilen bilgisayarlar anti-virüs, kişisel güvenlik duvarı ve diz üstü bilgisayarda sabit disk şifreleme yazılımı kurulu ve etkinliği pasif hale getirilemeyecek ve ayarları değiştirilemeyecek şekilde teslim edilir.

Güvenlik yazılımları, "Zararlı Yazılım Yönetimi Yönetmeliği" uyarınca zararlı yazılımlara karşı tehdit güncellemelerini ve periyodik taramalarını otomatik olarak yapar. Koruma yazılımları merkezi olarak izlenir ve kullanıcının bilgisayarlarında fark edilen tehditler ve güvenlik olaylarıyla ilgili kullanıcı bilgilendirilir ve BSGM tarafından tehdidi giderici aksiyonlar alınır.

Kişisel bilgisayarlar Windows işletim sistemi yazılımları güncellenmiş şekilde teslim edilir ve yeni yamalar işletim sistemine otomatik olarak yüklenir. BSGM tarafından test edilmiş ve onaylanmış işletim sistemi ve uygulama yamaları BSGM "Yama Yönetimi Talimatı"'na göre yüklenir.

İşten ayrılmalar veya şirket değişiklikleri İnsan Kaynakları tarafından BSGM'ye düzenli olarak bildirilir ve BSGM kullanıcı yönetim prosedürleri gereği gerekli aksiyonları alır.

1.4 Kişisel bilgisayarlarda kullanıcı hesaplarına normal kullanıcı seviyesinde yetki verilir. Kişisel bilgisayarlarda yüksek seviyeli kullanıcı yetkisi, kullanıcı tarafından doldurulmuş, kullanıcının bağlı olduğu yöneticisi ve varsa yerel Bilgi Sistemleri sorumlusu tarafından onaylanmış "Yerel Bilgisayarda Yüksek Seviyeli Kullanıcı Yetkisi Talep Formu" aracılığıyla talep edilebilir ve talep edilen yetki BSGM Bilgi Güvenliği Yöneticisi onayıyla, sadece geçerli iş gereksinimleri doğrultusunda verilebilir. Yetki verilen kullanıcılar BSGM tarafından periyodik olarak gözden geçirilir. Yetkinin verilebilme kriterleri ilgili talep formunda belirtilmiştir.

1.5 Kurulumla gelen veya onaylı yazılımlar dışındaki yazılımlar (lisanslı/lisanssız, tedarikçilerce demo amaçlı sağlanmış) bilgisayarlara yüklenemez. İş gereği yazılım yüklenmesi Bilgi Sistemleri Genel Müdürlüğü'nün onayı doğrultusunda gerçekleştirilebilir. BSGM kullanıcı bilgisayarlarını onaylanmamış ve lisanssız yazılımlar için periyodik olarak tarar ve yazılımları kaldırır.

1.6 Kullanıcı bilgisayarları, taşınabilir veri depolama cihazlarına (CD, DVD, taşınabilir sabitdisk, bellek, vb…) veri yazılamaz şekilde kullanıcıya teslim edilir. Taşınabilir veri ortamlarından kullanıcı bilgisayarlarına aktarılan veri güvenlik yazılımlarınca taranır. İş gereği taşınabilir veri depolama ünitelerine veri yazılması yetkisi "Taşınabilir Veri Cihazlarına Veri Yazma Yetkisi Talep Formu" ile talep edilebilir ve ancak BGK onayıyla verilebilir. Yetki verilen kullanıcılar BSGM tarafından periyodik olarak gözden geçirilir. Yetkinin verilebilme kriterleri ilgili talep formunda belirtilmiştir.

1.7 Kullanıcı, Şirket bilgisayarındaki veriyi gerektiği sıklıkta ortak alan klasörlerine yedeklemekten sorumludur. Ortak alanlar BSGM tarafından düzenli olarak yedeklenmektedir. Kullanıcılar kendi ortak alanlarının yetki yönetim sorumluluğunu BSGM'den devralma talebinde bulunabilirler.

1.8 Şirket bilgisayarlarıyla Şirket sistemlerine uzaktan erişim güvenliği, şifreleme ile sağlanmış iletişim mekanizmaları kullanılarak yapılır, başka yöntemler kullanılamaz. Bağlantı koşulları " Dışarıdan Şirket Bilgi Ortamlarına Erişim Yönetmeliği"nde tanımlanmıştır.

1.9 Kullanıcı bilgisayarıyla Şirket ağına bağlıyken aynı anda başka ağlara(misafir ağları, hot-spot, halka açık, 3. parti ağlar, vb…) bağlanamaz.

1.10 Çalışanlar Şirket bilgisayarıyla Şirket kaynaklarına (e-mail, iş uygulamaları, portaller, vb…) bilgisayarlarında yer alan güvenli bağlantı yazılımlarıyla erişebilirler.

Kuruma ait olmayan bilgisayarlardan (şahsi bilgisayarlar, internet cafe gibi ortak alan bilgisayarları vb.) kurum kaynaklarına uzaktan erişim yapamazlar.

2. Mobil Cihazlar:

2.1 Çalışanlar BSGM'nin kabul ettiği kriterlere uyan mobil cihazlarıyla BSGM'nin izin verdiği sistemlere belli bilgi güvenliği koşullarını gerçekleştirip bağlanabilirler. Bu koşullar "Mobil Cihaz ve Mobil Çalışma Yönetmeliği"nde belirlenmiştir.

2.2 Mobil cihazların Şirket sistemlerini kullanabilmesi için, cihazlarda gereksinim duyulan güvenlik ayarları ağ üzerinden otomatik yapılır. BSGM tarafından belirlenmiş mobil cihaz yönetim yazılımları yüklenir.

2.3 Çalışanlar Şirket ağlarına bağlanmış mobil cihazların fiziksel güvenliğinden sorumludur. Cihazın çalınması veya kaybolması durumunda BSGM'ye acilen bildirmesi gerekmektedir.

Bilgi ve Bilgi Ortamları Güvenliği

Kapsam: Şirket çalışanlarının kullandıkları bilginin gizliliğini, bilginin tutulduğu ve iletilebildiği ortamların güvenliği konusunu kapsar.

3. Bilgi Gizliliği Sınıflandırma

3.1 Şirket sistemlerinde ve kullanıcı bilgisayar ve cihazlarında tutulan dijital ve yazılı tüm bilgi, veri gizliliği sınıflandırmasına tabidir ve "Sınırlı Dağıtım", "Dahili" ve "Genel" olmak üzere üç seviyeye ayrılmıştır. Bilginin türüne göre gizlilik seviyesinin belirlenmesi "Bilgi Varlığı Sınıflandırma Rehberi(EK-1)"'ne göre yapılacaktır.

3.2 Kullanıcı bilgisayarlarında oluşturulan dosyaların gizlilik seviyesi, "Bilgi Varlığı Sınıflandırma Rehberi(EK-1)"'nde belirtilen kriterler yardımıyla kullanıcı tarafından belirlenir ve ilgili yazılımlar yardımıyla dijital olarak etiketlenir. Belirlenmiş bilgi güvenliği seviyesinin doğruluğu kullanıcının sorumluluğundadır.

BSGM, Şirket sistemleri ya da diğer kanallarla(internet, web mail, USB hafıza, cd-rom, vb...) iletilen verinin içeriğini bilgi sızmasına karşı tarar.

3.3 "Sınırlı Dağıtım" kategorisindeki Şirket bilgilerinin yüklü olduğu herhangi bir veri taşıma ortamının(CD, DVD, floppy disk, taşınabilir sabit disk yada USB bellek, vb…) kilitli olarak saklanması ve bu bilgileri içeren tüm ortamların şifre ile korunması gerekmektedir. Bilgi varlıklarının gizlilik seviyelerine göre saklama, yönetme ve iletme(3. şahıslara dahil) yöntemleri "Bilgi Varlığı İşleme Rehberi(EK-2)"'nde belirtilmiştir.

3.4 Şirket tarafından belirlenmiş ve onaylanmış Şirket servisleri dışında, İnternette ücretli yada ücretsiz veri depolama ve paylaşma hizmeti veren servislere veya sosyal medya sitelerine Şirket bilgisi(dosya, metin, resim, tablo, vb) yüklenmesi yasaktır. BSGM bu ortamlara Şirket ağlarından erişimi izlemektedir ve gerektiğinde engellemektedir.

3.5 Çalışanlar oluşturdukları her türlü yazılı (evrak, not, printer çıktısı, yazı tahtası, flipchart, vb…) ve dijital veri tutulan ortamların(cd-rom, USB disk, flash disk vb…), ürün ve ambalaj prototiplerinin, reklam ve afiş görseli gibi bilgi varlıklarının güvenliğinden sorumludur.

"Temiz Masa Politikası" gereğince çalışanlardan gün sonunda masalarında, printer ve fax makinalarında, ortak kullanım alanları ve toplantı salonlarında hiçbir bilgi varlığı bırakmamaları, dolap ve çekmecelerinde "Bilgi Varlığı işleme rehberi(EK-2)"'de belirtilen şekilde saklamaları beklenmektedir. BGK'ca görevlendirilen ekipler periyodik olarak çalışma alanlarının uygunluğunu "Temiz Masa Polikası" uyarınca kontrol eder.

Kullanılmayan yazılı bilgiler, sahipleri tarafından Şirket tarafından tahsis edilecek çapraz kesmeli kağıt öğütücüler tarafından yok edilir, normal çöp olarak atılmaz.

3.6 Farklı yerleşkeler arası herhangi veri barındıran ortamların(evrak, yedekleme kartuşu, bilgisayar/mobil cihaz, vb…) iletiminde Şirket içi kurye servisi ya da bilgi gizlilik koşullarımızla uyumlu ve onaylı kurye Şirketleri dışında herhangi bir servis kullanılamaz.

3.7 Tüm çalışanlar bilgi ortamlarının(kağıt, CD/DVD, tüm sabit diskler, hafıza kartları, USB bellekler, yedekleme teypleri, vb…) imhasında "Bilgi Ortamları İmha Standartları"nı izlemeleri gerekmektedir.

4. İnternet, Sosyal Medya kullanımı

4.1 Şirket ağlarına bağlı kullanıcı PC ve mobil cihazların internete erişim talebi yönetici onayına bağlıdır ve "İnternet Erişim Talep Formu" doldurularak talep edilir. Kullanıcılar internete, BSGM tarafından konumlandırılmış güvenlik sistemleri üzerinden erişirler.

Bütün kullanıcılar, bu tür servislere erişmeden önce internet proxy sunucularından geçerler ve erişimleri kayıt altına alınır. Yöneticiler, kendilerine bağlı çalışanların internet kullanımı raporlarını görüntüleme yetkisini "İnternet Kullanım Raporu Yetki Talep Formu" ile geçerli bir neden gösterilmesi koşuluyla isteyebilir. Bu raporlar bilgi güvenliği incelemelerinde kullanılabilir.

4.2 Kullanıcıların erişebileceği internet siteleri ve erişim koşulları "İnternet Kullanım ve Erişim Yönetimi Yönetmeliği"nde tarif edilmiştir. Erişimi kısıtlanmış sitelere erişim için gerekli yetkilendirme süreci bu yönetmelikte yer alır. Yasalarca ve BGK'ca erişimi yasaklanmış sitelere erişilemez.

4.3 Kişilerin herhangi bir sanal ortama web sitesine ya da sosyal medya paylaşım ortamına, Şirket kaynaklarından, yasalara aykırı, taciz edici, usandırıcı, inançlara saygısız, müstehcen, gözdağı verici, onur kırıcı, iftira niteliğinde, tehdit edici, küfürlü, yüz kızartıcı eylemlerde bulunması, yazılar yazması yada paylaşması yasaktır.

4.4 Şirket'in sosyal medya pazarlama aktiviteleri Dijital Medya Pazarlama departmanı tarafından yönetilir. Holding, şirketler ve markalar hakkında İnternet'te yazılanlar otomatik olarak taranarak belirlenir ve "Sosyal Medya Olay Yönetim Süreciyle" yönetilir.

5. E-mail ve Elektronik Haberleşme

5.1 Kullanıcıların uyması gereken e-posta kullanım kuralları "E-posta Kullanım Yönetmeliği"'nde açıklanmıştır.

5.2 Şirket içi çevrimiçi iletişimde Yıldız Holding tarafından sağlanan anlık mesajlaşma yazılımı kullanılır.

5.3 E-posta hizmetlerine erişim, Şirket bilgisayarlarına kurulu BSGM tarafından belirlenen e-posta yazılımıyla Şirket ağlarından ya da VPN yazılımıyla Şirket dışından Şirket ağlarına bağlanarak sağlanır. Kullanıcıların tarayıcıdan yapılan erişimle Şirket dışı bilgisayarlarına e-mail eklentisi indirmeleri ve bilgi aktarmaları uygun yazılımlarla izlenir.

5.4 Kişilerin e-posta kutularına başka kişilerce erişim koşulları "E-posta Kullanım Yönetmeliği "'nde tarif edilir. Erişim yetkisi "E-Posta Yetkilendirme Onayı" formuyla talep edilebilir ve değerlendirilmeye alınır.

Uygulama, Sistem ve Altyapı Güvenliği

Kapsam: Şirket çalışanlarının iş süreçlerini gerçekleştirmek için kullandıkları uygulama, sistem ve altyapının güvenliği konusunu içerir.

6. İş Uygulamaları Güvenliği

6.1 İş uygulamalarının operasyonel ve güvenlik yönetimi BSGM'nin sorumluluğundadır. Uygulamalar üzerinde iş birimleri çalışanlarınca oluşturulmuş verinin mülkiyeti ilgili iş birimlerinindir.

6.2 BSGM'nin onayı alınmadan Şirket ağlarından erişilebilir herhangi bir iş uygulaması tedarik edilemez ve kurulamaz, internetten servis olarak sağlanan yazılımlar(SaS) kullanılamaz.

BSGM kapsamında gerçekleştirilen iş uygulamaları projelerinin tasarım aşamasından canlıya alınmasına kadar olan süreçte gerçekleştirilmesi gereken teknik adımların uygunluğu "Proje Teknik Uygunluk Onayları Talimatı"na göre kontrol edilir.

Bütün iş sistemleri teknik ekipler tarafından "İş Uygulamaları Kurulum Yönetmeliği ve Standartları"nda belirtilen şekilde kurulur ve yönetilir. İş uygulamalarının üzerinde çalıştığı işletim sistemleri ve veri tabanları "Sunucu Kurulumu Yönetimi Talimatı" izlenerek kurulur.

İş uygulamaları ve üzerinde çalıştıkları işletim sistemleri ve veri tabanları zararlı yazılımlara ve ağ saldırılarına karşı BSGM tarafından izlenir ve gerekli önlemler alınır. Uygulamalarda tutulan veri, gizlilik seviyesine göre şifrelenerek saklanır.

6.3 BSGM, iş uygulamalarının kritikliğine göre bir felaket veya kesinti durumunda sistemlerin üzerinden yürütülen işlerin devamlılığını sağlamak için önlem ve tedbirleri alır.

İş uygulamaları ve tuttukları veriler "Yedekleme ve Geri Yükleme Yönetimi Talimatı"na uygun şekilde yedeklenir ve saklanır.

6.4 Bütün uygulamaların şifre standartları Holding "Parola Yönetimi Yönetmeliği"ne uymak zorundadır.

6.5 Normal ve yüksek seviyeli kullanıcı ve yetki yönetimi BSGM tarafından ilgili yönetmelikler izlenerek gerçekleştirilir. Uygulamalarda erişim yetkileri kişilerin iş fonksiyonlarına göre verilir.

6.6 Uygulamalara erişimler ve işlemler "Log Yönetimi Talimatı" göre Şirket tarafından kayıt altına alınır, standartlarda belirtildiği kadar saklanır ve gerektiğinde BSGM tarafından incelenir.

Sistemlerde gizli olarak belirlenmiş veriler ve bunlarla yapılan şüpheli işlemler gerek duyulursa kayıt altına alınabilir.

6.7 Sistemlerde yapılacak bütün yazılım değişiklikleri "Uygulama Değişiklik Yönetimi Yönetmeliği" izlenerek ilgili onay mekanizmalarına ve testlerine tabidir. Bilgi güvenliği mekanizmalarını etkisiz kılacak yada bypass edecek değişiklikler yapılamaz.

İş uygulamalarının test ortamları, canlı ortamdaki uygulamanın işleyişini ve verisini etkilemeyecek şekilde kurulur. Test ortamlarında canlı ortamlardan aktarılmış veriler "Test Verisi Oluşturma ve Yönetim Talimatı" izlenerek karartılır, gerçek veriyle eşleştirilemez hale getirilir.

6.8 İş uygulama yamaları, ilgili zayıflığın yarattığı riskler, uygulama fonksiyonları üzerine etkileri değerlendirilir, test sistemlerinde test edildikten sonra kurulur.

7. Sistem, Sunucu ve Ağ güvenliği

7.1 Şirket ağ mimarisi BSGM tarafından, izinsiz bağlantı girişimleri, saldırılar, zararlı yazılım erişimleri ve veri sızmalarına karşı en iyi uygulamalar ve standartlar doğrultusunda tasarlanır, ağ güvenliği birleşenleri ile korunur. Kablolu ve kablosuz ağ birleşenlerinin bağlantı erişim listeleri ve diğer ayarları iş uygulamalarının iletişim gereksinimleri doğrultusunda düzenlenir. İhtiyaç duyulmayan iletişim kanalları kapalı tutulur.

7.2 Şirket ağlarını izinsiz dinlemek, değişiklik yapmak, cihaz eklemek, kablosuz ağ erişim noktası oluşturmak, uzaktan erişim sağlamak, sunucu kurmak yasaktır. BSGM dönemsel olarak Şirket ağlarını onaysız değişiklik ve cihazlara karşı tarar.

7.3 Verinin gizlilik seviyesine göz önüne alınarak gerektiğinde iletim ya da depolanma aşamasında BSGM tarafından şifrelenebilir.

7.4 BSGM, sistemlerin ve altyapının kritikliğine göre bir felaket, arıza veya kesinti durumunda devamlılığını sağlamak için önlem ve tedbirleri alır.

7.5 Şirket sistemleri, sunucuları ve ağ birleşenleri BSGM tarafından belirlenmiş ortamlarda "Sistem Odaları Standartları Talimatı"'ıyla uyumlu ortamlarda saklanır. Dışardan alınan hizmetlerde tedarikçinin Şirket standartları seviyesinde fiziksel güvenlik önlemlerini ve çevresel kontrolleri karşılıyor olması ve ilgili maddeler düzenlenen servis anlaşmalarında yer alması beklenir.

7.6 Bütün sistemlerin şifre standartları Holding "Parola Yönetimi Yönetmeliği"'ne uymak zorundadır.

7.7 Tüm sistemler kurulurken, en iyi uygulamalar ve bilgi güvenliği standartları doğrultusunda ilgili platform için hazırlanmış "Güvenlik Ayarlarını Sıkılaştırma Rehberleri" izlenir. BSGM Bilgi Güvenliği ekibi tarafından güvenlik taraması ve zafiyet belirleme testleri yapılır.

7.8 İnternetten erişilebilen sunucular, sistemler, servisler ve ağ birleşenleri, BSGM Bilgi Güvenliği ekibi tarafından düzenli olarak taranır. Tespit edilen açıklıklar, zayıflıklar ve yama eksiklikleri belirlenir ve gerekli önlemler alınır.

7.9 İşletim sistemleri, veri tabanı sunucuları, ağ birleşenleri ve diğer birleşenlerin üreticileri tarafından yayınlanan yamalar, ilgili zayıflığın yarattığı riskler, sistemlerin fonksiyonları, üzerlerinde çalışan uygulamalar veya iletişim ağlarındaki yerleri değerlendirilir, test sistemlerinde test edildikten sonra kurulur.

7.10 Sistemlerde yüksek seviyeli kullanıcı yetkileri sadece sistem yönetiminden, güvenliğinden ve operasyonundan sorumlu kullanıcılara verilir. Danışman, programcı veya onaylanmamış dış kaynaklı sistem yöneticilerine yüksek seviyeli yetkiler verilmez. Dış kaynaklı tedarikçilerin sistemlerde yüksek seviyeli yetkilerle gerçekleştirdikleri işlemler kayıt altına alınır ve BSGM tarafında düzenli olarak incelenir.

Kullanıcılara işletim sistemi veya veri tabanı ortamına erişim izni verilmez.

8. Tedarikçi ve İş Ortaklarının Şirket Sistemlerine Erişimi

8.1 Şirket'e danışmanlık, yazılım/donanım kurulumu, bakım ve destek hizmeti veren, Şirket'in kaynak, veri, sistem ve ağlarına yerinde ya da uzaktan erişim sağlayan, bu ürün ve hizmetleri alt yüklenicilik yoluyla sunan tedarikçi ve iş ortakları, Şirketin bilgiyi işleme, saklama ve güvenliğiyle ilgili yönetmeliklere uymakla yükümlüdür.

8.2 Bu taraflar, Şirket'in kaynaklarına erişimleri onaylanmadan önce "Yıldız Holding Bilgi Sistemleri Gizlilik Sözleşmesi"'ni imzalamak zorundadır. Gizlilik Sözleşmesi'nin imzalanamadığı durumlarda, taraflarla yapılan sözleşmede gizlilik hükümleri yer almak zorundadır. Açıklanan ya da erişimi onaylanan bilginin gizliliği, hassaslığı, hacmi ve değeri açısından gerekli bulunması halinde, BSGM, ilave güvenlik önlemleri alınması talep edebilir.

8.3 Dış, üçüncü taraf ve iş ortakları ile yapılan sözleşmeler "Yıldız Holding Tedarikçi Sözleşmeleri Standartları"'na uygun hazırlanmalıdır. Dış, üçüncü taraf ve iş ortaklarından alınan hizmetten sorumlu olan Şirket çalışanları, iş ilişkilerinde ve yapılan sözleşmelerde, bilgi güvenliği yükümlülüklerinin yerine getirildiğinden emin olmalıdır.

8.4 Şirket'in kaynaklarına erişen dış ve üçüncü taraf kullanıcılarının işten ayrılması veya görev değiştirmesi gibi değişiklikler, BSGM'ye zaman geçmeden bildirilmelidir. Kullanıcı hesaplarının kapatılması ve yetkilerinin iptal edilmesi yönünde gerekli aksiyonlar alınmalıdır.

8.5 Şirket'e hizmet veren dış, üçüncü taraflar ve iş ortaklarına tahsis edilen kullanıcı yetkileri sadece gerektiğinde ve ihtiyaçlar doğrultusunda kullanılmalıdır, sistemlerin güvenliğine olumsuz etki edecek kullanımlarda bulunulmamalıdır. İhtiyaçlarla paralellik göstermeyen işlemler, tarafların yetkileri dahilinde olsa bile gerçekleştirilmemelidir.

8.6 Şirket'e hizmet veren dış, üçüncü taraflar ve iş ortakları, eriştikleri sistemler üzerindeki veri ve yazılımları, Şirket'in onayı olmadan başka veri ortamlarına kopyalayamaz ve kullanamaz. BSGM bu yönde gerekli önlemleri alır.

8.7 Dış ve üçüncü taraf kullanıcıları, Şirket tarafından ayrıca onay verilmemişse, holding kaynaklarına erişim için kuruma ait bilgi işlem cihazları kullanmak zorundadır.

9. Bilgi Güvenliği Olay yönetimi

Kapsam: Şirket'in bilgi güvenliği, bilgi gizliliği, bütünlüğü ve erişilebilirliğini, sistemleri ve iletişim ağlarını olumsuz şekilde etkileyebilecek bilgi güvenliği olaylarını yönetim konularını kapsar.

9.1 Bilgi güvenliği olaylarının yönetimi "Bilgi Güvenliği Olay Yönetim Planı"nda açıklanmıştır. Bilgi güvenliği olaylarından kaynaklanabilecek zararların en aza indirilmesi amaçlanır. Bilgi güvenliği olayları, Bilgi Güvenliği Olay Yönetim Takım Lideri tarafından yönetilir ve BGK'ya raporlanır.

9.2 Kullanıcılar gözlemledikleri bütün olayları ivedilikle Bilgi Sistemleri Yardım Masasına, yerel Bilgi Teknolojiler destek ekiplerine ya da bina güvenlik ekiplerine bildirmekle

yükümlüdür. Olayla ilgili yapılabilecek incelemelerde olay inceleme ekiplerine destek olmaları beklenmektedir.

10. Yönetmelik/Talimat Listesi

- Yama Yönetimi Talimatı
- Zararlı Yazılım Yönetimi Yönetmeliği
- Yedekleme ve Geri Yükleme Yönetimi Talimatı
- Test Verisi Oluşturma ve Yönetim Yönetmeliği
- Dışarıdan Şirket Bilgi Ortamlarına Erişim Yönetmeliği
- Mobil Cihaz ve Mobil Çalışma Yönetmeliği
- İnternet Kullanım ve Erişim Yönetimi Yönetmeliği
- Sosyal Medya Olay Yönetim Süreci
- E-Posta Kullanım Yönetmeliği
- Proje Teknik Uygunluk Onayları Talimatı
- İş Uygulamaları Kurulum Yönetmeliği
- Sunucu Kurulumu Yönetimi Talimatı
- Parola Yönetimi Yönetmeliği
- Log Yönetimi Talimatı
- Uygulama Değişiklik Yönetimi Yönetmeliği
- Güvenlik Ayarlarını Sıkılaştırma Rehberleri
- Yıldız Holding Bilgi Sistemleri Gizlilik Sözleşmesi
- Yıldız Holding Tedarikçi Sözleşmeleri Standartları
- Bilgi Güvenliği Olay Yönetim Planı
- Sistem Odaları Standartları Talimatı

Bilgi Varlığı Sınıflandırma Rehberi(EK-1)

Gizlilik Sınıfı	Açıklama	Örnek
Sınırlı Dağıtım	Şirket içinde sadece yetkili kişiler tarafından erişilen, kişiye özel ya da şirketin ticari başarısını etkileyebilecek hassas bilgilerdir.	Ticari ve endüstriyel sırlar, mali bilgiler, şirket stratejileri, AR&GE çalışmaları, çalışan özlük bilgileri, şifreler, denetim raporları…
Dahili	Şirket çalışanları tarafından erişilebilir bilgilerdir.	İç duyurular, politika, prosedürler, rehber bilgileri…
Genel	Şirket tarafından yayınlanmış, herkes tarafından erişilebilen bilgilerdir.	Basın bültenleri, hissedarlara duyurulan çeyrek raporları, iş ilanları…

Bilgi Varlığı İşleme Rehberi(EK-2)

	Yönetme			Saklama		İletme			
Gizlilik Sınıfı	**Erişim hakkı verme**	**Kopyalama**	**Elden çıkarma**	**Fiziksel olarak**	**Dijital olarak**	**Fiziksel olarak (iç ve dışa)**	**Dijital olarak**	**3. Şahıslara iletme**	**Faks**
Sınırlı Dağıtım	Yönetici izniyle	Sahibinin izniyle	Yönetici onayıyla, kağıt kırpma ya da güvenli silme (wipe)	Güvenli alanda, kilitli ortamda	Şifreli	Kapalı zarfta, güvenli kuryeyle kişiye özel, gönderi teyidi ve imzasıyla	Şifreli, yada şirket içi dosya transfer sistemini kullanarak	Yönetici onayı ve gizlilik sözleşmesi	Alıcı başında bekler
Dahili	Yönetici izniyle	Kısıtlama yok	Kısıtlama yok	İsteğe bağlı olarak kilitli	İsteğe bağlı olarak şifreli	İşaretleme yapılmamış zarfla	İstenirse şifrelenebilir	Gizlilik Sözleşmesi gerekmektedir	Kısıtlama yok
Genel	Kısıtlama yok	Kısıtlama yok	Kısıtlama yok	Kısıtlama yok	Şifrelenmez	İşaretleme yapılmamış zarfla	Şifrelenmez	Kısıtlama yok	Kısıtlama yok

REVİZYON TARİHİ	REVİZYON NO.	REVİZYON SEBEBİ
9 Nisan 2013	1	İlk Oluşturma
15 Mayıs 2013	2	Diğer politika linklerinin güncellenmesi
25 Eylül 2013	3	Gizlilik sınıflarında güncelleme, “temiz masa politikası” düzenlemesi, alt yönetmelik eklentileri