Komtaş Ekosistemi, Tâbi olduğu ulusal, uluslararası düzenlemeler, ilgili mevzuat ve standart gereksinimlerini, anlaşmalardan doğan yükümlülüklerini, iç ve dış paydaşlara yönelik kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimlerini sağlamak amacıyla ISO 27001:2022 Bilgi Güvenliği Yönetim Sistem Standardı (BGYS) 'nı ve ISO 27701 Kişisel Veri Koruma Yönetim Sistemini (KVYS) yaşatmayı ve 6698 sayılı Kişisel Verileri Koruma Kanuna (KVKK) uymayı hedeflemektedir.

Komtaş Ekosistemi kendilerinin ve paydaşlarının bilgi varlıklarına ve kişisel verilerini güvenli bir şekilde erişim sağlamayı, bilginin kullanılabilirliğini, bütünlüğünü ve gizliliğini korumayı, kendisinin ve paydaşlarının bilgi varlıkları ve kişisel verileri üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi, kurumun güvenilirliğini ve marka imajını korumayı, bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygulamayı, tabi olduğu ulusal, uluslararası veya sektörel düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmeyi, anlaşmalardan doğan yükümlülüklerini karşılamayı, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamayı, iş / hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmayı ve işin sürekliliğini ve sürdürülebilirliğini sağlamayı, kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi taahhüt eder.

Komtaş Ekosistemi, bu amaç doğrultusunda aşağıdaki hususları başarmayı taahhüt etmektedir;

a) KOMTAŞ ekosistemi çalışanları ve ilgili paydaşlarının BGYS ve KVYS farkındalıklarını artırmaya yönelik eğitim faaliyetlerini düzenlemek, KVKK (Kişisel Verileri Koruma Kanunu) kapsamında alınacak teknik ve idari tedbirler kapsamında eğitmek,

b) Sürekli ve sistematik değerlendirme ve geliştirmeyi etkin kılmak,

c) BGYS ve KVYS / KVKK çerçevesini desteklemek ve güvenlik politikasını periyodik olarak gözden geçirmek,

d) Üst yönetim liderliğinde gerekli görevlendirmeleri, atamaları ve kaynak tahsisini sağlamak,

e) Risk değerlendirmesi ve risk yönetimi esaslı sürdürülebilir bir Bilgi Güvenliği ve Kişisel Veri Yönetim sistemi uygulamak,

f) KVKK kapsamında veri envanterinin oluşturulması, Kurumsal politika prosedürlerin KVKK ya göre güncelenmesini sağlamak (Veri işleme ve saklama politikası, imha politikası, bilgi güvenliği politikası, özel nitelikli veri politikası vs.) ve KVKK kapsamında tüm idari ve teknik tedbirleri uygulamayı ve 6698 sayılı kanuna uymayı https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf ,

g) Aydınlatma metinlerinin (çalışanlar ve 3. Kişiler için) gözden geçirilmesi,

h) VERBİS kaydının güncellenmesi,

i) Müşteri ve diğer paydaşlar ile olan hizmet alma ve verme süreçlerinde Bilgi Güvenliği ve Kişisel veri mahremiyeti yükümlülüklerini dikkate alarak iş yapmak,

j) Başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak bağlamında Türkiye ve Avrupa Birliği Üye ülke kanunlarına uyum içinde kişisel verileri toplamak ve işlemek,

k) Kişisel verilerin işlenmesi konusunda; hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel; belirli, açık ve meşru amaçlar güderek; amaçla bağlantılı, sınırlı ve ölçülü bir biçimde kişisel veri işleme faaliyetinde bulunmak,

l) Kanunlarda öngörülen veya kişisel veri işleme amacının gerektirdiği süre kadar kişisel verileri muhafaza etmek,

m) Kişisel veri sahiplerini aydınlatmak ve kişisel veri sahiplerinin bilgi talep etmeleri durumunda gerekli bilgilendirmeyi yapmak,

n) Özel nitelikli kişisel verilerin işlenmesi bakımından öngörülen düzenlemelere uygun hareket ederek ve kanunlarda açıkça öngörülen haller dışında açık rıza olmaksızın fiil ve faaliyet gerçekleştirmemek,

o) Kişisel verilerin aktarılması konusunda kanunda öngörülen düzenlemelere uygun hareket ederek fiil ve faaliyet gerçekleştirmek,

p) Yasal ve düzenleyici gereksinimleri ve müşteri sözleşmelerine ilişkin güvenlik yükümlülüklerini dikkate alacak şekilde hizmeti sağlamak,

q) Kendisi ve paydaşlarının, çalışanlarının bilgi varlıklarına ve kişisel veri içeren sistemlere güvenli bir şekilde erişim sağlamayı,

r) Sorumlusu olduğu kişisel ve kurumsal bilgilerin kullanılabilirliğini, bütünlüğünü ve gizliliğini korumayı,

s) Kendisinin ve paydaşlarının bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi,

t) Kurumun güvenilirliğini ve marka imajını korumayı,

u) Bilgi güvenliği ve Kişisel Veri ihlali durumunda gerekli görülen yaptırımları uygulamayı, 72 saat süresi içinde KVKK ya bildirimde bulunmayı, Bilgi güvenliği ve KVKK ilgili tüm yasal mevzuat ve sözleşmelere uyulması için mümkün olan en kısa sürede ve kesintisiz olarak hizmetlerimizi sunmayı,

v) TS ISO/IEC 27001 ve 27701 BGYS & KVYS standardının gereklerini yerine getirecek şekilde kurulan kontrol altyapısı ile bilgi güvenliği ve kişisel verilerin mahremiyat seviyesini korumayı ve iyileştirmeyi,

w) Kaynakların tahsis edilmesini, kurulmasını, işletilmesini ve sürekli iyileştirilmesini,

x) Gerçekleştirilen bilgi güvenliği ve KVKK çalışmalarının yasalara ve standartlara uygunluğunu tespit etmek için iç denetimler ve bağımsız 3. Taraf kurumlar tarafından denetlenmeyi,

Taahhüt eder.