Bu politika, Sisoft Sağlık Bilgi Sistemleri A.Ş'nde bulunan bütün birimlerdeki personelin, bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Sisoft bünyesinde kurulan Bilgi Güvenliği Yönetim Sistemi (BGYS), Sisoft varlıkları ve Sisoft tarafından yürütülen faaliyetlerin güvenliğini sağlamak amacıyla kurulmuştur.

Sisoft, şirket bünyesinde yürütülen veya yürütülecek projelerin mevcut ya da oluşturulacak tüm faaliyetlerine ilişkin bilgilerin güvenliğini sağlamayı, iş sürekliliğini en az kesinti ile sağlamayı, şirkete ait ve korumakla yükümlü olduğu üçüncü taraflara ait tüm bilgilerin gizliliğini temin etmeyi, iş süreçleri ve hizmetlerin sürdürülmesinde kullanılan her türlü fiziksel ve elektronik bilgi varlıklarının Gizlilik, Bütünlük ve Erişilebilirlik kriterleri doğrultusunda korunmasını hedefler.

Sisoft, Bilgi varlıklarına erişen ve kullanan tüm çalışanlar, tedarikçiler, iş ortakları ile diğer tüm üçüncü taraflar;

- Bilgi Güvenliği Politika, Prosedür ve Talimatlarına uygun davranmalıdır,
- Kuruma ait bilgilerin gizliliğini sağlamalı, işlediği bilgiyi yedeklemelidir,
- Sistemin geliştirilmesi için uygun gördüğü öneri ve geliştirmeleri ilgililere iletmelidir,
- Güvenlik ve olay ihlallerini sorumlu birime bildirmelidir.

Sisoft ve çalışanları olarak, iş sürekliliğimize ve bilgi varlıklarımıza yönelik her türlü riski yönetmek amacıyla;

- TS ISO/IEC 27001 Standardına uygun şekilde Bilgi Güvenliği Yönetim Sisteminin kurulumunu, gerçekleştirilmesini, işletilmesini, izlenmesini, gözden geçirilmesini, bakımını ve sürekli iyileştirilmesini,
- BGYS amaçları belirlenerek bu amaçların gerçekleştirilmesi için gerekli planın yapılmasını,
- Bilgi güvenliği ile ilgili tüm yasal mevzuat ve sözleşmelere uyulmasını,
- Varlık ve süreçler üzerindeki risklerin analizleri yapılarak, analizlerin sonuçlarına bağlı olarak risk değerlendirmelerini ve risk kriterlere ortaya konularak bu çerçevede risk yönetiminin sistematik olarak sağlanmasını,
- Riskleri kabul etme ölçütlerini ve kabul edilebilir risk seviyelerini belirlemek üzere gerekli çalışmaların organize edilmesi ve yönetilmesini,
- Bilgi Güvenliği Yönetim Sistemi çerçevesindeki yenilikler, değişimler ve gelişmelerin tüm çalışanlar ve paydaşların farkındalıklarını sağlayacak şekilde duyurulmasını,
- Tüm kuruluşta bilgi güvenliği farkındalığının oluşturulmasını,
- Yılda en az bir kez BGYS Politikasını gözden geçirmeyi ve gerekli görüldüğü hallerde düzenlemeleri yaparak ilgili taraflara duyurulmasını taahhüt ederiz.