BİLGİ GÜVENLİĞİ HİZMET SÖZLEŞMESİ

Bir tarafta Orman Genel Müdürlüğü (kısaca OGM) ile diğer tarafta HİZMET ALINAN FİRMANIN ADRESİ adresinde bulunan HİZMET ALINAN FİRMANIN ADI (kısaca "FİRMA KISA ADI") arasında aşağıdaki şartlarda bilgi güvenliği hizmet sözleşmesi imzalanmıştır.

1- Güvenlik gereksinimlerinin analizi ve özelleştirilmesi

Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Ortaya konan güvenlik gereksinimleri bilgi varlıklarının değerini ve bir güvenlik açığı dolayısıyla oluşabilecek zararı yansıtmalıdır. Sistem geliştirilirken işin başından itibaren güvenlik ihtiyaçları göz önünde bulundurulmalıdır.

2- Girdi verilerinin kontrolü

Uygulama sistemlerine veri girişi doğru olduğundan emin olmak için doğrulanmış olması gerekmektedir. Kontroller veri girişi için(isim ve adresleri, vatandaşlık numaraları, vb) ve parametre tablolar (fiyat, para birimi dönüştürme oranları, vergi oranları, vb) alanlarına uygulanmalıdır.

Aşağıdaki kontroller dikkate alınmalıdır:
1) Giriş kontrolleri aşağıdaki hataları tespit etmelidir.
1.1) Limiti aşan(out-of-range) değerleri;
1.2) Veri alanlarında geçersiz karakterler;
1.3) Eksik veri;
1.4) Yetkisiz veya tutarsız kontrol verileri;
2) Anahtar alan veya veri dosyalarının geçerliliklerini ve bütünlükleri periyodik olarak gözden geçirilmelidir.
3) Uygulama dökümantasyonu izinsiz değişikliklerden korunmalıdır (tüm giriş belgeleri değişiklikleri izinli olmalıdır)
4) Doğrulama hataları için prosedürler olmalıdır;
5) Giriş verisinin inandırıcılığını için prosedürler;
6) Veri giriş sürecine dâhil olan tüm personelin sorumluluklarını tanımlı olmalıdır.

3- İç işleyişin kontrolü

Kontroller uygulamanın doğasına göre ve vereceği iş etkisine göre olmalıdır.

Aşağıdaki kontroller uygulanmalıdır.

1) Oturum ve erişimlerden sonra verilerdeki güncellemeler kontrol edilmelidir.
2) Son kontrol edilen verilere göre açılan veriler son açılmış halleri ile dengelenmeli ve kontrol edilmelidir.
3) Sistem tarafından oluşturulan verinin doğruluğu kontrol edilmelidir.
4) Ana sunucu ve istemciler arasında ki verinin trafiği esnasında verinin bütünlüğü kontrol edilmelidir.

5) Sistem de kayıtların ve dosyaların hash değerleri kontrol edilmelidir.
6) Programların doğru saat ayarları ile çalıştığı kontrol edilmelidir.
7) Fonksiyon ve programların doğru sırada çalıştığı kontrol edilmeli, sıra bozulduğunda işlemler kesilmelidir.

4- Mesaj bütünlüğü

Elektronik veri içeren mesajların taşınması esnasında izinsiz değişimi ve bozulmasına karşın kontroller kullanılmalıdır. Mesaj bütünlüğünü sağlamak için donanımsal veya yazılımsal herhangi bir algoritma kullanılabilir. Mesaj bütünlüğü kritik olan tüm verilerin transferi için sağlanmalıdır. Mesajın yetkisiz erişim ve değiştirilmesinin önlenmesi için kriptografik teknikler kullanılmalıdır.

5- Çıktı verilerinin kontrolü

Uygulama sisteminden depolanan bilginin veri çıkışı doğru ve uygun olduğu doğrulanmış olmalıdır. Sistem çıktıları uygun doğrulama, onay ve test işlemlerinden geçtikten sonra düzgün istenilen çıktıyı oluşturmalıdır.

Sistem çıktıları için
1) Çıktıların güvenilir olduğuna dair makul kontrolleri içermelidir.
2) Girdi ve çıktı verileri arasında uzlaşma kontrolleri tüm sistem işlemlerini karşılamalıdır.
3) Bir okuyucu ya da sonraki işleme sistemi için doğruluğu, eksiksizliği, hassaslığını, sınıflandırılmasını sağlamalıdır.
4) Çıkış bilgisi doğrulama testleri için prosedürler olmalıdır;
5) Veri çıkış sürecine dahil olan tüm personelin sorumluluklarını tanımlı olmalıdır.

6- Kriptografik Kontroller

Kritik Bilginin yetkisiz kişiler tarafından erişilmemesi, değiştirilmemesi ve güvenliğinin sağlanması için kriptografik kontroller kullanılmalıdır.

Kripto grafik kontrollerin uygulanması için sistem içerisindeki verilerin kritiklik düzeyleri belirlenmeli ve bu sistem için tespit edilen risklere göre kontrollerin uygulanmasına karar verilmelidir. Bu konuda firmanın kripto grafik kontrollerin kullanımına dair bir politikası olmalıdır. Bu politikaya göre karar vermelidir.

Şifreleme bilginin gizliliğini korumak için kullanılabilecek bir tekniktir. Hassas bilgilerin korunması için düşünülmelidir. Bir risk değerlendirmesine göre, koruma gereken düzeyde bilgileri şifreleme firmanın şifreleme politikasına göre şifre uzunluğu ve algoritma belirlenerek karar verilmelidir.

Dijital imzalar özgünlük ve bütünlüğünü korumanın bir yolu olarak kullanılmalıdır. Dijital imzalar elektronik ticaret gibi uygulamalarda verinin kim tarafından imzalandığını ve verinin imzalandıktan sonra değişikliğe uğramasını kontrol etmek için kullanılmalıdır.

Elektronik ticaret işlemlerinde ödemelerde de elektronik imza kullanılmalıdır. Elektronik imza içi gizli imzanın güvenliği sağlanmalıdır. İmza sahibi ve bu imzayla imzalanmış verilere erişen kişiler dışında erişim engellenmelidir.

Elektronik imza uzunluğu ve kullanılan algoritma ile ile ilgili iyileştirmeler düzenli olarak iyileştirilmelidir. Şifreleme için kullanılan anahtarlar dijital imzalarda kullanılanlardan farklı olmalıdır.

7- Çalışmakta olan yazılımın denetimi

Çalışan sistemlere yazılım yüklenmesini bozulma riskini asgariye indirmek için prosedürler oluşturulmalıdır. Yazılım yükleme, eğitimli sistem yöneticileri tarafından ve sadece yönetim yetkilendirmesi ile yapılmalıdır. Çalışan sistemde geliştirilmekte olan yazılım ve derleyici bulunmamalıdır. İşletim sistemi ve uygulama yazılımlarının iyice test edilmeden yüklenmemelidir. Konfigürasyon kontrol sistemi aracılığı ile eski ve yeni yazılım sürümleri, yazılımla ilgili dokümantasyon ve konfigürasyon bilgileri ve sistem dokümantasyonu bulunmalıdır.

8- Sistem test verilerinin korunması

Test verileri korunması için gerekli kontroller alınmalıdır. Sistem test verisi gerçek sistemdeki veri ile boyut ve içerik olarak kabul edilebilir düzeyde yakın olmalıdır. Kişisel bilgilerin bulunduğu veriler, test verisi olarak kullanılmamalıdır. Kişisel veri kullanılacaksa kullanılan veri kişisel gizli bilgi içeriğinden çıkarılmalıdır.

Eğer gerçek sistemdeki operasyonel veri test için kullanılacak ise aşağıdaki kontrollere dikkat edilmelidir.

1) Sistem verilerine uygulanan erişim politikası aynen test verisine de uygulanmalıdır.
2) Operasyonel sistem verisinin test sistemine kopyalanması aşamasında yetki kontrolleri uygulanmalıdır.
3) Test işlemi bittikten sonra test verisi hemen silinmelidir.
4) Operasyonel sistem verisinin kopyalanması kayıt altına alınmalıdır.

9- Program kaynak kütüphanesine erişimin kontrolü

Uygulamaların zarar görmemesi için, program kaynak kütüphanelerine erişim kısıtlanmalıdır.
1) Mümkün olan durumlarda kaynak kütüphane operasyonel sisteme konulmamalıdır.
2) Çalışan personelin tüm kaynak kütüphaneye erişimi olmamalıdır.
3) Geliştirme ve bakım esnasındaki programların sınırsız bir şekilde operasyonel kaynak kütüphaneye erişimi engellenmelidir.
4) Kaynak kütüphanede yapılacak değişiklikler için personel kurum içinde uygun olan yönetimi onayını almalıdır.
5) Programlama listeleri güvenilir ortamlarda tutulmalıdır.
6) Kaynak kütüphanelerine tüm erişimler kayıt altına alınmalıdır.
7) Eski sürümleri, anlaşılır bir şekilde arşivlenmiş olmalıdır. Arşivlerde kesin tarih ve saatleri ne zaman operasyonel olduğu, destek bilgileri, iş kontrolü, veri tanımları ve prosedürler bulunmalıdır.
8) Kaynak kütüphanelerde yapılacak bakım işlemlerinde önceden tanımlanmış kontrollerin değişmemesine dikkat edilmelidir.

10- Değişim kontrol prosedürleri

Bilgi sistemleri üzerinde yapılacak değişiklikler resmi kontrol prosedürleri aracılığı ile denetlenmeli ve yeni sistem ilaveleri ve büyük değişiklikler resmi bir belgeleme, tarif, test ve kalite kontrol süreci uyarınca gerçekleştirilmelidir.

11- İşletim sistemi değişiklerinin ardından uygulamaların teknik olarak gözden geçirilmesi.

İşletim sisteminde yapılan değişikliklerin ardından kritik uygulamaların gözden geçirilip test edilmesini sağlayan süreç veya prosedürler olmalıdır. Değişiklik gerçekleştirilmeden belli bir zaman önce ilgili yerlere haber verilerek test ve gözden geçirmelerin yapılması sağlanmalıdır.

12- Yazılım paketlerinde yapılacak değişikliklerin kısıtlanması

Yazılım paketleri üzerinde değişiklik yapılması gerçekten gerekli olduğu durumlar dışında engellenmelidir. Hazır yazılımlar mümkün olduğu sürece değiştirilmeden kullanılmalıdır. Değişikliğin kaçınılmaz olduğu durumlarda Programın gömülü kontrollerine ve bütünlüğüne ilişkin süreçlerin tahrip edilmemesine, değişiklik sonucunda yazılımın bakımının kuruluş tarafından sürdürülmesi gerekirse bu durumun kabul edilebilir olup olmadığının değerlendirilmesine dikkat edilmelidir.

13- Yazılım Geliştirme

Yazılım geliştirme faaliyetleri lisans anlaşması, fikri mülkiyet hakları, kalite güvencesi, Denetleme için erişim hakkı, kurulum öncesi zararlı kod araması için test hususları izlenmeli ve denetlenmelidir.

14- Yasal gereksinimlere uyum

Her bir bilgi sistemi için ilgili bütün yasal, düzenleyici ve sözleşmeye bağlı gereksinimler ve gereksinimleri sağlamak için kullanılacak kurumsal yaklaşım açık şekilde tanımlanmalı ve belgelenmelidir. Bu gereksinimleri karşılamak amacıyla kontroller ve bireysel sorumluluklar tanımlanmalı ve belgelenmelidir.

Kullanılmakta olan yazılım ve diğer her türlü materyal ile ilgili olarak yasal kısıtlamalara uyulması açısından kopya hakkı, düzenleme hakkı, ticari marka gibi hakların kullanılmasını güvence altına alan prosedürler olmalıdır. Bu prosedürler uygulanmalıdır. Fikri mülkiyet olabilecek materyalin korunması için aşağıdaki hususlara özen gösterilmelidir.

1) Kullanım haklarının çiğnenmemesi için yazılımın sadece güvenilir kaynaklardan sağlanması.
2) Mülkiyet haklarını ispatlamak için delil olarak kullanılabilecek lisans sözleşmesi, orijinal disk, kullanıcı rehberi vb. materyalin muhafaza edilmesi.
3) Azami kullanıcı sayısının ihlal edilmemesini sağlamak için tedbirler alınması.
4) Yazılım ve diğer ürünler için sadece lisanslı versiyonların kullanıldığının kontrollerle denetlenmesi.

15- Kurumsal kayıtların korunması

Organizasyonun önemli kayıtları kanun, kontrat, anlaşma ve işin doğasından kaynaklanan gereksinimler uyarınca kaybolmaya ve bozulmaya karşı korunmalıdır. Kayıtların saklanması için kullanılan ortamın zaman içinde bozulabileceği göz önünde bulundurulmamalıdır.

Veri saklama sistemi seçilirken belli bir süre sonra teknoloji değişikliği dolayısıyla kayıtların okunamaz hale gelmemesi için gerekli tedbirler alınmalıdır. Donanımsal ve yazılımsal format uyumunu sağlamak için gerekli program ve teçhizat kayıtlarla birlikte saklanmalıdır.

16- Uzaktan çalışma

Uzaktan çalışma faaliyetleri için organizasyonun güvenlik politikasına uygun plan ve prosedürler geliştirilmelidir. Uzaktan çalışmanın yapılacağı yerde ekipman ve bilginin çalınmasına, bilgiye yetkisiz erişim yapılmasına, kuruluşun dahili sistemlerine uzaktan yetkisiz erişime ve bilgi işlem araçlarının kötüye kullanılmasına engel olmak için önlemler alınmalıdır. Uzaktan bağlantılarda kurumun firmaya verdiği hesaplar için sorumlu firmadır. Bu hesapların ortak kullanımı engellenmelidir.

17- Uygulama Erişimi Denetimi

Erişim kontrolü politikası uyarınca kullanıcılar ve destek personeli için bilgilere erişim kısıtlanmalıdır. Kullanıcıların bilgiyi yazma, okuma, silme, değiştirme veya çalıştırma hakları düzenlenmelidir.

18- Duyarlı Sistem Yalıtımı

Uygulamanın duyarlılığı uygulama sahibi tarafından açıklanmalıdır. Duyarlı bilgilerin bulunduğu sistemler diğer sistemlerden izole edilmelidir.

19- Elektronik ticaret güvenliği

Elektronik ticaret internet gibi açık ağlar ile kurum arasında olan elektronik posta iletişimi gibi tüm elektronik veri alışverişini içermektedir. Elektronik ticaret için ağ tehditleri, hileli etkinlik, sözleşme bilginin yetkisiz ele geçirilmesi veya değiştirilmesi gibi birçok tehditle karşı karşıyadır. Kontroller bu gibi tehditlerin gerçekleşmesini engellemek için uygulanmalıdır. Bu tür tehditler için kontroller aşağıdakileri içermelidir.

1)Müşteri gibi dışarıdan elektronik ticareti kullanan kişiler için kimlik doğrulama sağlanmalıdır.
2) Müşteri gibi dışarıdan elektronik ticareti kullanan kişiler için yetkiler verilmelidir.
3) Kritik sözleşme, doküman ve bilgilere erişim engellenmelidir.
4) Fiyatlandırma bilgilerinden gizli olanlar korunmalıdır.
5) Sipariş işlemleri için teslimat adresi bilgileri, ödeme bilgileri gibi kritik bilgilerin güvenilirliği ve bütünlüğü korunmalıdır.
6) Müşteri tarafından ödeme onay işlemleri olmalıdır.
7) Dolandırıcılığın engellenmesi için ödeme şekilleri çeşitlendirilmelidir.
8) Ödeme işlemleri için fonksiyon sıralaması kontrol edilmeli ikilenen işlemlerin olması engellenmeli ve sıralama bütünlük ve gizliliğe göre tasarlanmalıdır.

9) Hileli işlemler için sorumlu tespit edilmeli, sorumluların tespit edilmediği durumlarda, sorumluluk uygulamanın sağlandığı firmalarda olmalıdır.

10) Kripto grafik kontroller elektronik ticaret uygulamaların da mutlaka kullanılmalı ve düzenli olarak güncel teknolojilere göre sıkılaştırılmalı ve güncellenmelidir.

Yukarıda ki kontroller kriptografik işlemler ve yasal zorunluluklara uyum ile kapatılabilir.

20- "On-line" işlemler

"On-line" işlemlerle ilgili bilgi hatalı gönderme, hatalı yönlendirme, mesajın yetkisiz kişiler tarafından ifşa edilmesi, değiştirilmesi, kopyalanması veya tekrar gönderilmesine karşı korunmalıdır.

21- Halka açık bilgi

Halka açık bilginin bütünlüğü yetkisiz kişilerin değişiklik yapmaması için korunmalı. Sistem üstünde teknik açıklık testleri yapılmalıdır. Halka açık sisteme konmadan önce bilginin onaylanmasını sağlayan belgelenmiş bir süreç olmalıdır.

22- Olay kayıtlarının tutulması

Erişimi gözlemek ve gerektiği takdirde soruşturmalarda kullanmak üzere gerekli sistemlerde kullanıcı faaliyetleri güvenlik ile ilgili olay kayıtları tutulmalıdır ve bu kayıtlar 6 ay boyunca saklanmalıdır.

Kullanıcı kimlikleri, oturuma giriş ve çıkış tarihleri ve zamanları, eğer mümkünse terminal kimliği, başarılı ve reddedilmiş sistem erişim denemeleri, sistem konfigürasyonunda yapılan değişiklikler, ayrıcalıkların kullanılması, hangi dosyalara erişimin gerçekleştiği ile ilgili kayıtlar tutulmalıdır.

Sistem yöneticilerinin kendi faaliyetlerini silme yetkisine sahip olmaması gerekmektedir.

23- Bilgi ve Yazılım Değiş Tokuşu

Her türlü iletişim ortamında bilginin güvenliğini sağlamak için resmi bir değiş tokuş politikası veya prosedürü uygulanmalıdır.

24- Uygulama ve Veritabanı hesapları

Uygulama ve veritabanın da firma hesaplarıyla yapılan tüm işlemlerden firma sorumludur. Hesapların firma içerisinde kullanılması ve hesap şifre güvenliği firmaya aittir. Veritabanı kullanıcı yönetiminden firma sorumludur.

25- GENEL HÜKÜMLER

25.1 İşbu sözleşme içerisindeki maddelerin tamamına uyulması zorunludur. OGM buradaki maddelerden herhangi birinin kontrolünü istediği zaman isteyebilir. Bu maddelere uyulamamasından doğacak her türlü olayda sorumlu ilgili firmadır.

25.2. İşbu Sözleşme'ye yapılacak tüm tadiller yazılı olarak yapılacak ve her iki tarafça imzalanacaktır.

25.3. İşbu Sözleşme hükümlerinden biri veya birkaçının, herhangi bir kanun veya düzenleme altında geçersiz, yasadışı ve uygulanamaz ilan edilmesi durumunda geride kalan hükümlerin geçerliliği, yasallığı ve uygulanabilirliği bundan hiçbir şekilde etkilenmez veya zarar görmez.

25.4. Taraflardan birinin iş bu Sözleşme'nin herhangi bir şekilde karşı tarafça ihlalinden doğan bir hakkını, yetki veya gücünü kullanmaması veya ertelemesi, iş bu sözleşmedeki herhangi bir haktan vazgeçmesi anlamına gelmez veya bu hakkın daha sonra kullanmasını veya işbu Sözleşme'nin müteakip ihlallerinde diğer hak, yetki ve çözümlerini kullanmasına engel teşkil etmez.

25.5. İşbu Sözleşme hükümlerinden yapılan herhangi bir feragat veya hak sahibinin hiçbir onayı yazılı olarak yapılmadıkça geçerli kabul edilemez.

25.6. İşbu Sözleşme'nin uygulanması veya yorumuyla ilgili uyuşmazlıklarda, haklılığı sabit olan Taraf'ın yaptığı makul harcamalar, ödemeler ve vekâlet ücretini diğer taraf'tan tahsil etme hakkı saklıdır.

25.7. Taraflar, mahkemelerinin münhasır yargılama yetkisini kabul ederler.

25.8. Tarafların yukarıda belirtilen adresleri yasal ikametgâh adresleri olup; adres değişikliği yazılı olarak karşı tarafa bildirilmediği sürece bu adreslere yapılacak tebligatlar kanunen geçerli bir tebligatın bütün sonuçlarını doğuracaktır.

İşbu sözleşme, bu madde ile birlikte toplam 25 ana maddeden ibaret olup, düzenlenmesine ihtiyaç duyulan diğer koşullar bu sözleşmeyle çelişmeyecek şekilde düzenlenip, sözleşmeye eklenecek ve bu sözleşmenin ayrılmaz bir parçası olacaktır. Bu sözleşme, taraflarca ..... Tarihinde imzalanmış ve aynı gün yürürlüğe girmiştir.

Orman Genel Müdürlüğü **HİZMET ALINAN FİRMA**

…….Dairesi Başkanlığı