FARUK ÇUBUKÇU – ISO 27001 EĞİTİMİ

FC-YAZILIM GELİŞTİRME ŞİRKETİ

ISO 27001 KONTROLLERİ - UYGULANABİLİRLİK BİLDİRGESİ (STATEMENT OF APPLICABILITY)

ÖRNEK BİR ÖN ÇALIŞMA

A.9 Fiziksel ve çevresel güvenlik				
A.9.1 Güvenli alanlar				
Numara	Açıklama	Kayıt Gerektiriyor mu?	Uygulanabilir mi?	Uygulanabilirliğin İfadesi
A.9.1.1	Fiziksel güvenlik çevresi	EVET	EVET	Bilgi İşlem odası ve Server odasına giriş/çıkış kart kontrollü olacaktır. Giriş/çıkış kayıtları, Kartlı Geçiş kontrol sistemi üzerinde loglanacaktır.
A.9.1.2	Fiziksel giriş kontrolleri	EVET	EVET	Kartlı Geçiş kontrol sistemi üzerinde; özel erişim kontrol modu ile bilgi işlem ve server odasına girebilecek personel tanımlanır. Giriş/çıkış kayıtları, Kartlı Geçiş kontrol sistemi üzerinde loglanacaktır.
A.9.1.3	Ofisler, odalar ve olanakları için korumaya alma	EVET	EVET	Yazılımcı odalarına giriş/çıkış kart kontrollü olacaktır. Giriş/çıkış kayıtları, Kartlı Geçiş kontrol sistemi üzerinde loglanacaktır. Resepsiyon masası ise yüksek ve iç bölüme geçişi engelleyecek şekilde tasarlanmıştır.
A.9.1.4.	Dış ve çevresel tehditlere karşı koruma	HAYIR	EVET	Binanın yangın alarmı mevcuttur. Isıya duyarlı su fıskiyeleri vardır. 2. Katta olduğumuz için sel riski yoktur. Deprem ve diğer tehlikeler için İl Sivil Savunma kurumundan eğitim alınmış ve görev dağılımı yapılmıştır.
A.9.1.5	Güvenli alanlarda çalışma	HAYIR	HAYIR	Yukarıdaki maddelerin dışında güvenli alan kullanılmamaktadır.
A.9.1.6	Açık erişim, dağıtım ve yükleme alanları	HAYIR	HAYIR	Dağıtım ve yükleme alanı kullanılmamaktadır.
A.9.2 Teçhizat güvenliği				
A.9.2.1	Teçhizat yerleştirme ve koruma	HAYIR	EVET	Server odası kabinetler ve özel elektrik donanımlarına sahiptir. Kullanıcı bilgisayarları ve yazıcıları özel tasarım büro masalarına monte edilmiştir.
A.9.2.2	Destek hizmetleri	HAYIR	EVET	Tüm şirket, bilgi işlem odası ve server odası yeterli UPS ile beslenmektedir. Destek hizmetleri bir tedarikçi firma ile yapılan anlaşma ile sağlanmaktadır.

				Aksaklıklara karşı tazminatlar içeren maddeler vardır.
A.9.2.3	Kablolama güvenliği	HAYIR	EVET	Şirket yerel ağı yapısal kablolama sistemiyle veri, ses ve elektrik prizleri sağlar. Sistem hataya toleranslı (fault tolerant) olarak tasarlanmış ve uygulanmıştır.
A.9.2.4.	Teçhizat bakımı	EVET	EVET	Destek hizmetleri bir tedarikçi firma ile yapılan anlaşma ile sağlanmaktadır. Garanti kapsamında düzenli bakımlar düzenli olarak yapılmakta. Bu çalışmalar donanım envanterine bağlı olarak loglanmaktadır.
A.9.2.5	Kuruluş dışındaki teçhizatın güvenliği	HAYIR	HAYIR	Şirketimizde dışarıya donanım çıkarılmamaktadır.
A.9.2.6	Teçhizatın güvenli olarak elden çıkarılması ya da tekrar kullanımı	EVET	EVET	Süresi dolan ya da arızalanan depolama ortamları özel olarak bu konuda çalışan uzman bir firma tarafından yerine getirilmektedir. Yapılan çalışmalar donanım envanterine bağlı olarak loglanmaktadır.
A.9.2.7	Mülkiyet çıkarımı	EVET	EVET	Özel durumlarda donanım ve yazılımın bulunduğu yerden çıkarılması şirket müdürünün yetkisiyle yapılmaktadır. Bu amaçla form mevcuttur.
A.10 Haberleşme ve işletim yönetimi				
A.10.1 Operasyonel prosedürler ve sorumluluklar				
A.10.1.1	Dokümante edilmiş işletim prosedürleri	EVET	EVET	İşletim prosedürleri şirketimizin portalında bulunmakta ve yetki tanımlamalarına uygun olarak bütün kullanıcıları kendilerini ilgilendiren uygulamaların prosedürlerine erişebilmektedirler. FÇ Doküman yönetimi standartlarına göre yönetilen portalımızda dokümanların düzenli olarak güncellenmektedir.
A.10.1.2	Değişim yönetimi	EVET	EVET	Değişim Yönetimi, bütün değişiklikler için standard prosedürlerle sağlanır. Maliyet, fayda ve riski hesaplanan değişiklikler onaylanarak uygulanır. Ayrıca yapılan bütün değişiklikler loglanır.
A.10.1.3	Görev ayrımları	HAYIR	EVET	Belli görevler, birbirini kontrol edecek şekilde farklı kişiler tarafından yerine getirilerek ve düzenli denetleme yapılarak kontrol edilir.
A.10.1.4	Geliştirme test ve işletim	HAYIR	EVET	Geliştirme ekibi, satış, destek ve yönetim ekibi ayrı alt ağlar kullanırlar.

	olanaklarının ayrımı			Bkz: FÇ Ağ ve alt ağ tasarımı şeması.
A.10.2 Üçüncü taraf hizmet sağlama yönetimi				
A.10.2.1	Hizmet sağlama	EVET	EVET	Yapılan hizmet anlaşmalarında; bizim güvenlik ve işletim standardlarımızı karşılamak üzere özel maddeler yer almaktadır.
A.10.2.2	Üçüncü taraf hizmetleri izleme ve gözden geçirme	EVET	EVET	Alınan destek ve bakım hizmetleri her ay yapılan denetimlerle kontrol edilir. Olağan, çağrı bazlı ve diğer hizmetler izlenir. Bu çalışmalar loglanarak geçmişe dönük olarak da kontroller yapılır.
A.10.2.3	Üçüncü taraf hizmetlerindeki değişiklikleri yönetme	HAYIR	EVET	Alınan destek ve bakım hizmetleri gelişmelere göre değişecek şekilde esnek yapılır.
A.10.3 Sistem Planlama ve kabul				
A.10.3.1	Kapasite planlama	EVET	EVET	Donanım ve yazılım envanteri kullanım değerleriyle takip edilir ve altı aylık projeksiyonlar yapılır.
A.10.3.2	Sistem kabulü	EVET	EVET	Yazılım ekibi ve diğer ekiplerden alınan yeteri kadar üye ile oluşturulan değerlendirme ekibi; kendi gereksinimlerini karşılamak için gerekli sistem özelliklerini (bellek kapasitesi, işlemci hızı, yazılımların performansı gibi) yeni alınacak sistemler üzerinde test ederler.
A.10.4 Kötü niyetli ve mobil koda karşı koruma				
A.10.4.1	Kötü niyetli koda karşı kontroller	HAYIR	EVET	Her ay üçüncü taraflarca yapılan penetrasyon testleri gerekli saptama işlemini içermektedir. Onun dışında kullanıcıların kötü niyetli kodlara karşı yapabilecekleri önlemler ve kurtarma çalışmaları yapılan iç eğitimlerle anlatılmaktadır.
A.10.4.2	Mobil koda karşı kontroller	HAYIR	EVET	Gereksinim duyulan mobil kodlar sistem kurulumu sırasında sağlanır. Onun dışında gereksinim duyulan mobil kodların sisteme yüklenmesi işletim sistemi politikalarıyla engellenir.
A.10.5 Yedekleme				
A.10.5.1	Bilgi yedekleme	EVET	EVET	Yazılım geliştirme ve idari kullanıcıların verileri ve yazılımları düzenli olarak yedeklenir. Alınan yedekler her ay düzenli olarak geri yüklenerek sağlam olup olmadıkları kontrol edilir. Bu çalışmalar tutulan loglarla desteklenir.

A.10.6 Ağ güvenliğinin yönetimi				
A.10.6.1	Ağ kontrolleri	EVET	EVET	Yerel ağ ve dış ağlar (Internet) bağlantısı, firewall aracılığıyla kontrol edilmektedir. Site ve chat programları gibi standart güvenlik kurallarının yanı sıra saldırı tespitleri yapılır ve loglanır. Misafir kullanıcılar için bir seferlik süre kısıtlı şifreler verilerek kablosuz bağlantı yapması sağlanır.
A.10.7.1	Ağ hizmetleri yönetimi	EVET	EVET	Ağ hizmetleri; güvenlik özellikleri ve hizmet seviyeleri olmak üzere tanımlanır. Buna uygun olarak, ağ hizmetleri tedarikçi bir firma tarafından sağlanır. Yapılan anlaşmalar altı ayda bir gözden geçirilir.