ÇARŞAMBA
TİCARET VE SANAYİ ODASI
BİLGİ GÜVENLİĞİ POLİTİKASI

İçindekiler

SUNUŞ

Günümüzde her kurumun ve kuruluşun bir bilgi işlem sistemi mevcuttur ve kurumsal işlemler bu sistem içerisinde yürütülmektedir. Hizmetlerin hızı ve aynı standartlarda hizmet üretimi dolayısıyla da müşteri memnuniyeti bilgi işlem sistemi ile doğrudan ilişkilidir. Bu durum hizmetin verildiği bilgi işlem sisteminin güvenli, verimli ve riskli durumlarda acil tedbirleri kullanabilme kabiliyetini hayati önem seviyesine getirir ki, bu da kurumların bu konuda kendi ihtiyaç ve önceliklerine cevap verecek politika üretmesini ve bunu sürekli işler halde tutmasını gerektirir. Uygunsuz ve standart dışı kullanımlar Odamızı virüs saldırılarına, ağ sistemlerinin çökmesine, dolayısı ile verilmekte olan hizmetlerin aksamasına sebep olabilir ve bunlar yasal sorumluluklar ile karşı karşıya kalınmasına neden olabilir.

Tüm çalışanlarımızı bağlayacak olan bu politikanın unsurları Odamızın ihtiyaç ve önceliklerine göre aşağıdaki şekilde belirtilmiştir.

Genel Kurallar

Odamız bünyesinde oluşturulan tüm veriler Odanın mülkiyetindedir. Çalışanlar bilgi sistemlerinden, kendi kişisel kullanımları için sınırlı seviyede yararlanabilirler.

- Odamız bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.
- Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
- Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.
- Odamız Bilgi İşlem Sistemi Danışmanlık firmasının bilgisi olmadan, Oda Ağ sisteminde (web hosting servisi, eposta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.
- Odamız Bilgi İşlem Sistemi Danışmanlık firmasının bilgisi olmadan, bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vb. üzerinde mevcut yapılan düzenlemeler hiçbir surette değiştirilmemelidir.
- Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.
- Dizüstü bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Asla özel bilgiler bulunmamalıdır.
- Çalışanlar bilinmeyen kimselerden gelen e-postaları açarken çok dikkatli olmalıdırlar. Çünkü bu e-postalar virüs ve Truva atı gibi zararlı programları barındırabilirler.
- Çalışanların şifrelerini başkalarına vermesi kesinlikle yasaktır.
- Kişisel Verilerin Korunması Kanunu kapsamında getirilen yükümlülükler ile süreç özelinde KVKK uyumu sağlanmalıdır.

1. İnternet Erişim ve Kullanım Politikası

- İhtiyaç doğrultusunda içerik filtreleme sistemleri kullanılacaktır.
- İstenilmeyen siteler yasaklanabilecektir.
- Anti-virüs gateway sistemleri kullanılmalıdır. Sertifikaların güncelliği takip edilmelidir. İnternete giden veya gelen bütün trafik virüslere karşı taranmalıdır.
- Çalışma saatleri içerisinde aşırı bir şekilde iş ile ilgili olmayan sitelerde gezinmek ve işlem yapmak yasaktır.
- Bilgisayarlar üzerinden genel ahlak anlayışına aykırı Internet sitelerine girilmeyecek ve dosya indirimi yapılmayacaktır.
- İnternet üzerinden Odamız tarafından onaylanmamış yazılımlar indirilemez ve Oda sistemleri üzerine bu yazılımlar kurulamaz.
- Odamızın işlevlerine yönelik yazılım ihtiyaçları için ilgili prosedürler dâhilinde ilgili birim sorumlularına müracaat edilmesi gerekmektedir.
- Üçüncü şahısların Odamız internet ağını kullanmaları Genel Sekreterliğin veya yetkilendirdiği kişinin izni ve bu konudaki kurallar dâhilinde gerçekleştirilebilecektir.

2. Ağ Yönetimi Politikası

- Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için özel kontroller uygulanmalıdır.
- Ağ servisleriyle ilgili standartlarda, erişimine izin verilen ağlar ve ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmelidir. Ağ üzerinde kullanıcının erişeceği servisler kısıtlanmalıdır.
- Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitIerine otomatik olarak bağlanması sağlanmalıdır.
- Sınırsız ağ dolaşımı engellenmelidir.
- Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmalıdır.
- Ağ bağlantıları periyodik olarak kontrol edilmelidir.
- Gerek görülen uygulamalar için elektronik posta, tek yönlü dosya transferi, çift yönlü dosya transferi, etkileşimli erişim, güne ve günün saatine bağlı erişim gibi uygulama kısıtlamalarıyla ağ erişimi denetimi yapılmalıdır,
- Ağ üzerindeki yönlendirme kontrol edilmelidir.

3. Şifre Politikası

- Bütün sistem seviyeli şifreler en az üç ayda bir değiştirilmelidir.
- Bütün kullanıcı seviyeli şifreler en az altı ayda bir değiştirilmelidir.
- Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.
- Oda çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.

- Şifrelerin ilgili kişiye gönderilmesi "kişiye özel" olarak yapılmalıdır.
- Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır.

4. E-Posta Politikası

- Odamız e-posta sistemi, taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.
- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- Odamız ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bu kapsama eklenen öğeler de dahildir.
- Kişisel kullanım için Internet'teki sitelere üye olunması durumunda Odamıza ait e-posta adresleri kullanılmamalıdır.
- Kullanıcıların, kullanıcı kodu/şifresini girmesini isteyen e-postaların, sahte e-posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
- Oda çalışanlarının kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır. Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.
- Oda personeli tarafından Internet ortamı aracılığı ile iletilen her türlü kişisel e-posta mesajının altında e-posta iletisinin içeriğinden ve niteliğinden Odanın sorumlu tutulamayacağı gibi açıklamalar yazılmalıdır.
- Çalışanlar, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Bu yüzden şifre kullanılmalı ve e-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

5. Anti-Virüs Politikası

- Odanın bütün PC tabanlı bilgisayarları anti-virüs yazılımına sahip olmalıdır ve belli aralıklarda düzenli olarak güncellenmelidir. Buna ek olarak anti-virüs yazılımı ve virüs parterleri otomatik olarak güncellenmelidir. anti-virüs yazılımı sertifikalarının güncelliği takip edilmelidir.
- Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır.
- Bilinmeyen kişilerden e-posta ile birlikte gelen dosya veya makrolar kesinlikle açılmayacaktır. Bu tür e-postalar ve ekleri hemen silinecek, daha sonra "silinmiş öğeler" klasöründen de tekrar silinecektir.
- Bilinmeyen veya şüpheli kaynaklardan asla dosya indirilmeyecektir.
- Bilinmeyen kaynaklardan gelen, USB bellekleri ve CD-ROM'lar virüslere karşı tarama yapılmadan kullanılmayacaktır.
- Kritik data ve sistem konfigürasyonlarını düzenli aralıklar ile yedeklenecek ve güvenli bir yerde saklanacaktır.

6. Uzaktan Erişim Politikası

- Uzaktan erişim için yetkilendirilmiş Oda çalışanları veya Odanın bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

- Internet üzerinden Odanın herhangi bir yerindeki bilgisayar ağına erişen kişi veya firmalar VPN teknolojisini kullanacaklardır. Veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlanması için bu şarttır.
- Uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme veya güçlü bir uzun şifre destekli public/private key sistemi kullanılması şeklinde olacaktır.
- Oda çalışanları hiç bir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler.
- Odanın ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.
- Uzaktan erişim yöntemi ile Odamıza erişen bütün bilgisayarlar en son güncellenmiş anti-virüs yazılımına sahip olmalıdırlar.

7. Risk Değerlendirme Politikası

Odamızın bilgi işlem ağında sistem açıklarını tespit etmek ve gerekli tedbirlerin alınmasını sağlamak amacıyla yetkili firma veya bilgi işlem sorumlusu tarafından, risk analizi yaptırılmasına dair kuralları içeren politikadır.

- Risk analizi çalışması süresince çalışanlar gerekli noktalarda yardımcı olacaklardır.
- Risk değerlendirme raporları Odaya elden teslim edilecek ve rapor, söz konusu risk ve hassasiyetler giderilene dek bilgi işlem sisteminde çevresel ve fiziksel güvenlik önlemleri alınmış bir ortamda saklanacaktır.
- Risk değerlendirme çalışmalarına başlamadan önce çalışma kapsamına konu sistemler ve çalışma süreleri Odaya bildirilecek ve bu çalışmalar Oda tarafından izlenecektir.
- Risk değerlendirme çalışmaları esnasında sistemler üzerinde servis reddi veya herhangi bir sebeple iş sürekliliği aksatılmayacaktır.

8. Acil Durum Yönetimi Politikası

Odamız bilgi işlem sistemine yapılabilecek direkt saldırılar, zararlı kod içeren programların, kişilerin sisteme sızması, bilginin hırsızlığı, dışarıdan veya içeriden gerçekleştirilebilecek saldırılar öncesi yapılması gereken aksiyonları tanımlayan politikamızdır.

- Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.
- Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır.
- Odamız bilişim sistemlerinin kesintisiz çalışmasını sağlaması için aynı ortamda kümeleme uzaktan kopyalama, yerel kopyalama, pasif sistem çözümlerini hayata geçirilebilir.
- Oda bilgi işlem sistemlerini tasarlarken ne kadar süre iş kaybını tolere edeceklerini göz önüne almalıdırlar.
- Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
- Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
- Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.

Acil Durum kapsamında değerlendirilen olaylar aşağıda tanımlanmıştır

Seviye A: Bilgi kaybı. Odamıza ait değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi

Seviye B: Servis kesintisi. Oda hizmetlerinin kesintisi veya kesintisine yol açabilecek durumlar

Seviye C: Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.

- Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin Odamıza getireceği kayıplar ve bu riskler oluşmadan önce ve oluştuktan sonra hareket planları tanımlanacak ve dokümante edilecektir.
- Acil durumlarda Odamız Bilgi İşlem Sistemi Danışmanlık firması yetkilisine ulaşılabilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
- Odamız Bilgi İşlem Sistemi Danışmanlık firması yetkilisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.
- Olayın türü ve boyutuna göre emniyet veya diğer Kurumlara başvurmak gerekebilir. Bu Özel olaylar (hırsızlık vb), başvurulacak Kurumlar, başvuru şekli (telefon, dilekçe vb),başvuruyu yapacak Oda yetkilisi önceden belirlenmiş ve dökümante edilecektir.

9. Bilgi İşlem Sistemi Yedekleme Politikası

Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve verilerin düzenli olarak yedeklenmesi gerekmektedir.

- Verinin operasyon el ortamda online olarak aynı disk sisteminde farklı disk volümlerinde ve offline olarak Manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır.
- Taşınabilir ortamlar (Manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya kiralanacak banka kasasında güvenli bir şekilde saklanmalıdır.
- Veriler offline ortamlarda en az 10 (on) yıl süreyle saklanmalıdır.
- Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
- Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyon el prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunması gerekir.
- Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı,ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme

sırasında sorunlar çıkarsa nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerli ligi periyodik olarak gözden geçirilmelidir.

- 2 server tarafından günlük yedeklemeler dahili harddiske alınmalıdır. Ayda bir tüm bilgisayarların hard disk kopyalaması yapılmalıdır. Harddiskler banka kasasında ve oda kasasında muhafaza edilmelidir.

10. Bakım Politikası

Odamız sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımları, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.