1. Kullanıcı Hesabı ve Erişim Yönetimi

BT departmanı, şirketin dijital sistemlerine güvenli erişimi sağlamakla yükümlüdür. Yeni bir çalışanın işe başlaması durumunda, ilgili yöneticinin talebi üzerine kullanıcı hesabı oluşturulur. Kullanıcı hesaplarına rol bazlı erişim yetkileri atanır. Bu yetkiler, çalışanın görev tanımına uygun şekilde belirlenir.

Erişim taleplerinde yetkisiz erişimi önlemek için çok katmanlı doğrulama yöntemleri kullanılır. Çalışan pozisyon değiştirdiğinde veya işten ayrıldığında erişim yetkileri derhal güncellenir ya da kapatılır. Tüm erişim işlemleri sistem loglarında kayıt altına alınır.

2. Şifre Politikaları ve Güvenlik Kuralları

Bilgi güvenliğini sağlamak için güçlü şifre politikaları uygulanır. Çalışanlar, sistemlere giriş yaparken karmaşık şifreler kullanmak zorundadır. Şifreler en az 8 karakterden oluşmalı, büyük/küçük harf, rakam ve özel karakter içermelidir. Şifrelerin 90 günde bir yenilenmesi zorunludur.

BT departmanı, şifre güvenliği ihlallerini önlemek amacıyla kullanıcıları düzenli olarak bilgilendirir. Şifrelerin yazılı veya üçüncü kişilerle paylaşılması kesinlikle yasaktır. Olağan dışı erişim denemeleri tespit edildiğinde sistem otomatik olarak hesabı kilitler ve BT ekibine uyarı gönderir.

3. Donanım ve Ekipman Talep Süreci

Yeni donanım veya ekipman talepleri, ilgili yöneticinin onayıyla BT departmanına iletilir. Talep edilen ekipmanlar stok durumuna göre tahsis edilir veya satın alma süreci başlatılır. Tüm ekipmanlar zimmet karşılığı kullanıcıya teslim edilir ve envanter sistemine kaydedilir.

Arızalanan veya eskimiş cihazlar için kullanıcı, BT destek ekibine arıza kaydı açar. İnceleme sonucunda cihaz onarılır ya da yenisiyle değiştirilir. Kullanıcı, teslim ettiği ekipmanla ilgili tüm veri ve bilgilerin güvenli şekilde silindiğinden emin olmalıdır.

4. Yazılım Lisanslama ve Kurulum Süreçleri

BT departmanı, şirket genelinde kullanılan tüm yazılımların lisanslarını takip eder. Lisanssız veya yetkisiz yazılım kurulumu yasaktır. Talep edilen yazılımlar, BT birimi tarafından güvenlik ve uyumluluk açısından kontrol edilir, ardından kurulum yapılır.

Yazılım güncellemeleri, güvenlik açıklarını kapatmak ve performansı artırmak için düzenli aralıklarla uygulanır. Kullanıcılar kendi başlarına yazılım yükleyemez; bu işlemler yalnızca BT personeli tarafından gerçekleştirilir.

5. Bilgi Güvenliği Politikaları ve Veri Koruma

BT departmanı, şirket verilerinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için bilgi güvenliği politikalarını uygular. Tüm çalışanlar bu politikalara uymakla yükümlüdür. Hassas verilerin taşınması veya paylaşılması durumunda şifreleme yöntemleri kullanılır.

Veri kaybını önlemek için düzenli yedekleme prosedürleri uygulanır. Yetkisiz veri erişimi, kopyalama veya dışa aktarım girişimleri güvenlik sistemleri tarafından izlenir. Gerektiğinde BT ekibi anında müdahale eder ve ilgili yöneticileri bilgilendirir.

6. Yardım Masası (Helpdesk) ve Destek Süreci

BT departmanı, kullanıcıların teknik sorunlarını çözmek için yardım masası hizmeti sunar. Çalışanlar, e-posta, portal veya telefon aracılığıyla destek talebi oluşturabilir. Tüm talepler öncelik durumuna göre sınıflandırılır ve mümkün olan en kısa sürede çözülür.

Destek süreçleri standart prosedürlere göre yürütülür ve her işlem kayıt altına alınır. Sık yaşanan sorunlar için BT portalında “Sıkça Sorulan Sorular” bölümü bulunur. Bu sayede kullanıcılar birçok sorunu kendi başlarına çözebilir.

7. Ağ (Network) Yönetimi ve Erişim Kuralları

BT departmanı, şirketin ağ altyapısını yönetir ve kesintisiz erişimi garanti altına alır. Tüm ağ cihazları güvenlik duvarı ve IDS/IPS sistemleriyle korunur. Kullanıcıların ağa erişimi kimlik doğrulama süreçlerinden geçtikten sonra sağlanır.

Kablosuz ağ erişimi yalnızca yetkilendirilmiş cihazlara açıktır. Ziyaretçiler için ayrı bir misafir ağı bulunur ve bu ağ, şirket ağıyla tamamen izole edilmiştir. Ağ trafiği düzenli olarak izlenir ve anormallikler BT güvenlik ekibi tarafından analiz edilir.

8. Siber Güvenlik ve Tehdit İzleme Prosedürleri

Şirketin BT altyapısı, siber tehditlere karşı 7/24 izlenmektedir. Güvenlik duvarları, antivirüs yazılımları, IDS/IPS sistemleri ve SOC (Security Operations Center) altyapısı üzerinden anlık uyarılar takip edilir. Şüpheli aktiviteler tespit edildiğinde öncelikli müdahale prosedürü devreye alınır.

Çalışanlar da sosyal mühendislik saldırılarına karşı bilgilendirilir ve düzenli olarak farkındalık eğitimlerine katılır. Kimlik avı (phishing) veya kötü amaçlı yazılım şüphesi durumunda kullanıcıların BT ekibini derhal bilgilendirmesi beklenir.

9. Sistem Yedekleme ve Felaket Kurtarma Planı

BT departmanı, kritik sistemlerin düzenli olarak yedeklenmesini sağlar. Yedekler hem yerel hem de bulut ortamında güvenli şekilde saklanır. Sistem çökmesi veya veri kaybı durumunda felaket kurtarma planı devreye alınır ve sistemler kısa sürede yeniden çalışır hale getirilir.

Felaket kurtarma testleri yılda en az bir kez yapılır. Bu testlerle süreçlerin etkinliği değerlendirilir ve gerekli iyileştirmeler yapılır. Böylece olası bir kriz anında iş sürekliliği kesintiye uğramadan devam ettirilir.

10. Uzaktan Çalışma ve VPN Kullanım Prosedürleri

Uzaktan çalışan personelin sistemlere güvenli erişimi için VPN (Virtual Private Network) altyapısı kullanılır. VPN erişimi yalnızca yetkilendirilmiş kullanıcılar için aktif edilir. Girişlerde çok faktörlü kimlik doğrulama zorunludur.

Uzaktan çalışma esnasında kişisel cihaz kullanımı yasaktır; yalnızca şirket tarafından sağlanan cihazlar kullanılabilir. Tüm uzaktan bağlantılar BT departmanı tarafından loglanır ve gerektiğinde denetlenir. Güvenlik ihlali tespit edilmesi durumunda bağlantı derhal kesilir.