

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

BİLGİ TRANSFERİ PROSEDÜRÜ (BTP)

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme		
Bilgi Güvenliği Yönetim Müdürü	Bilgi Sistemleri ve Teknolojileri Daire Başkanı	Genel Sekreterlik Temsilcisi

Doküman Kod	IKU-BSTDB-BTP-001	Revizyon Tarihi	
Yayın Tarihi	24.01.2022	Revizyon No	BTP-001-1.0

İÇİNDEKİLER

1. AMAÇ VE KAPSAM	3
2. İLGİLİ DOKÜMANLAR	3
3. UYGULAMA	3
3.1. Bilgi Transferi	3
3.2. Kurum İçi Bilgi Transferi	3
3.3. Kurumlar arası / Müşteri / Üçüncü Taraflar ile Bilgi Transferi.....	4
3.4. Fiziksel Bilgi Taşıma	4
3.5. Kurumsal E-posta hizmeti	5
3.6. Gizlilik ve İfşa etmeme Anlaşmaları Çerçevesi.....	5
3.7. E-fatura Uygulaması.....	6
3.8. Kayıtlı Elektronik Posta / Elektronik Tebligat Uygulaması	6
3.9. Web servisleri üzerinden bilgi paylaşma uygulaması	6
4. REVİZYON BİLGİSİ	7

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

Doküman Kod	IKU-BSTDB-BTP-001	Revizyon Tarihi	
Yayın Tarihi	24.01.2022	Revizyon No	BTP-001-1.0

1. AMAÇ VE KAPSAM

Bu prosedür, kurum içi ve kurum dışı olası bilgi alışverişinden kaynaklanacak risklerin önüne geçmek için gerekli kuralları tanımlamayı amaçlar. Bu prosedür, kurumdaki bilgi sistemlerini meydana getiren varlıkları, personeli, üçüncü tarafları ve iş süreçlerini kapsamaktadır.

2. İLGİLİ DOKÜMANLAR

No	İLGİLİ ARAÇLAR
1	İKÜ BSTDB Erişim Kontrol Politikasına
2	İKÜ BSTDB Felaket Kurtarma ve İş Sürekliliği Politikası
3	Genel Sekreterlik ve Yazı İşleri İş Akışları
4	İKÜ BSTDB Kurumsal Gizlilik Taahhütnamesi
5	Varlık Transfer Formu

3. UYGULAMA

3.1. Bilgi Transferi

T.C. İstanbul Kültür Üniversitesi, iç ve dış taraflar ile bilgi değişimini yazışmalar, web servisleri, elektronik iletişim, dosya paylaşımı ve medya transferi gibi farklı yollarla gerçekleştirmektedir. Bu değişim yöntemleri ile ilgili güvenlik kontrolleri ve uygulamaları aşağıdaki başlıklarda belirtilmiştir.

Yerleşkeler arasındaki bilgi / bilgi varlığı değişimleri, x bir dosyayı / formu teslimi güvenli bir hat üzerinde (VPN) yapılmaktadır.

3.2. Kurum İçi Bilgi Transferi

- Kurum birimleri arasındaki bilgi transferi elektronik ortamda iç yazışma esasına dayanır.
- Birimler arasında bilgi değişimi onayları üst birim yöneticisi seviyesinde verilir.
- Kurum içerisindeki yazışmalar, kurum teamüllerine uygun olarak sağlanır, saklanır ve imha edilir.
- Birimler çalışma alanı olarak dosya sunucusu üzerindeki ortak alanları kullanırlar. Bu sistem üzerinde yer alan dosya ve klasörlere erişim İKÜ BSTDB Erişim Kontrol Politikasına uygun olarak sağlanır.
- Dosya sunucusu dışında herhangi bir alan çalışma alanı olarak kullanılmaz. Dosya sunucusu üzerinde çalışılan ve iletilen dokümanların güvenliği İKÜ BSTDB Erişim Kontrol Politikasına, Genel Sekreterlik ve Yazı İşleri İş Akışları dokümanına ve İKÜ BSTDB Felaket Kurtarma ve İş Sürekliliği Politikasına uygun olarak sağlanır.

Gelen evraklar, Yazı İşleri İş Akışları dokümanına göre yapılmaktadır.

Doküman Kod	İKÜ-BSTDB-BTP-001	Revizyon Tarihi	
Yayın Tarihi	24.01.2022	Revizyon No	BTP-001-1.0

3.3. Kurumlar arası / Müşteri / Üçüncü Taraflar ile Bilgi Transferi

Kurum, diğer kurum ve kuruluşlar ile kritik bazı bilgi değişimleri gerçekleştirmektedir. Kurum, üçüncü taraflarla bu bilgi değişimi ve paylaşımını web servisleri, dosya paylaşımı, elektronik iletişim, uygulamalar, elden teslim vb. gibi farklı yöntemler ile gerçekleştirir.

1. Kurum ile diğer kurum ve kuruluşlar arasında, bilgi transferi / gönderilmesi / alınması için bir protokol/sözleşme yapılmış olması şartı aranır.
2. Bilgi transferleri için yapılan anlaşmalar, muhatap kurum ve kuruluşun sağladığı bir protokol/sözleşme metni ile de olabilir.
3. Anlaşmada bilgi transferi için başlangıç-bitiş tarihleri, bilgi transferinden sorumlu kişiler, bilgileri saklama, kullanım ve paylaşım koşulları, bilgi değişiminin nasıl gerçekleşeceği, ne tür güvenlik önlemlerinin alınacağı ve tarafların sorumlulukları belirtilir.
4. Bilgi transferinin güvenliği, protokol/sözleşmede belirtildiği şekilde gerek kurum gerekse üçüncü taraf tarafından sağlanır.
5. Bilgi transferi yapılmadan önce, transfer edilecek bilginin hassasiyet / kritikliği seviyesine göre Bilgi Güvenliği Yöneticisi tarafından şartlarını değerlendirir ve hassasiyet / kritiklik seviyesine bağlı olarak (gizli / çok gizli) transferi onaylar.
6. "Hizmete özel" ve daha düşük hassasiyetteki bilgi transferi için Bilgi Güvenliği Yönetici onayı aranmaz.
7. "Çok Gizli" bilgiler herhangi bir kişi veya kurum ile güvenli olmayan yöntemler ile paylaşılmaz. Kamu kurumu / Savunma Sanayi Başkanlığına bağlı kuruluşlarla bilgi paylaşımı fiziksel olarak gerçekleştirilir.
8. Kuruma ait bilgilerin diğer taraflarla paylaşılması tüm yasal, düzenleyici kurallar ve kurum politikaları ile uyumlu olmalıdır.
9. Özel olarak kişisel verilerin korunması, insan hakları ve genel gizlilik kurallarına uyulacaktır.
10. Transferde iletilen bilgilerin güvenliği sağlamak amacıyla, iletilen bilgilerin sınıfına göre şifreleme (encryption) teknikleri uygulanır.
11. Yazılım geliştirme hizmeti alınan 3. taraflar ile yapılacak bilgi değişiminde, bilgiye yetkisiz erişim ve yetkisiz ifşanın engellenmesi için, sözleşmelerde gizlilik maddelerine yer verilir ve İKU BSTDB Kurumsal Gizlilik Taahhünamesi imzalanır.

3.4. Fiziksel Bilgi Taşıma

1. Kurum, diğer kurum ve kuruluşlar ile bilgi transferini gerektiğinde basılı evrak, taşınabilir disk, cd/dvd, flash disk, taşınabilir depolama ünitesi, hafıza kartı vb. ortamlar aracılığıyla yapabilir.
2. Periyodik veya sürekli gerçekleştirilen bilgi transferi için yukarıda 2. maddede belirtildiği şekilde, taraflar arasında bilgi transferinin güvenliği için gerekli protokol / sözleşmenin yapılmış olması gerekir.

Doküman Kod	IKU-BSTDB-BTP-001	Revizyon Tarihi	
Yayın Tarihi	24.01.2022	Revizyon No	BTP-001-1.0

3. Ancak, seyrek veya tek seferlik yapılan fiziksel bilgi aktarımı (resmi yazı ile bilgi iletme, bilgi edinme taleplerine cevap verme vb.) için protokol / sözleşme yapılması şartı aranmaz.
4. Ancak bu tür bilgi transferi işlemlerinin güvenli olarak gerçekleştirilmesi için karşı tarafla görüşerek mutabakata varılır.
5. Taşıma işlemi öncesi bilgi transferi için Bilgi Güvenliği Yöneticisinin veya üst yönetimin onayı alınır.
6. Taşıma öncesi "Varlık Transfer Formu" doldurulur ve onaylatılır.
7. Onay verilmeyen taşıma işlemleri gerçekleştirilmez.
8. Taşınacak olan bilgi, taşıma ortamında mümkün ise şifreli / kilitli / görülemeyecek şekilde taşınmalıdır (şifreler sadece gönderen ve alacak olan taraflarda bulunmalıdır).
9. Taşıma işlemi bir kurye aracılığı ile yapılacaksa, bu kuryenin güvenlik taramasından geçmiş olması/Üçüncü Taraf Personeli Güvenlik Taahhünamesini imzalamış olması gerekir.

3.5. Kurumsal E-posta hizmeti

Kurumsal e-posta hizmeti Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı tarafından verilmektedir. Web üzerinden kullanıcılar e-postalarına ulaşabilmektedir. Exchange ActiveSync özelliği ile kullanıcılar, e-postalarına mobil cihazlardan da ulaşabilmektedirler. Elektronik mesajlaşma için sunucular ile istemciler arasında SSL sertifikası kullanılmaktadır.

1. Kurum dışı elektronik posta alış-verişinde SMTP protokolü kullanılmaktadır.
2. E-posta sunucusu tarafından sunulan OWA (Outlook Web Application), Outlook, Active Sync hizmetlerinin tamamında SSL sertifikası kullanılır.
3. Spam ve virüslere karşı SMTP gateway olarak Symantec Brightmail ürünü kullanılmaktadır.
4. Ayrıca Exchange sunucuları üzerinde saldırılara karşı güvenlik kuralları bulunmaktadır.
5. İç ve dış bağlantıları karşılayan ve e-posta trafiğini yöneten sunucular birbirleriyle yedekli olarak çalışmaktadır.

Kurum içi anlık mesajlaşma için MS Teams ürünü ile hizmet verilmektedir.

1. MS Teams üzerinde anlık mesajlaşma kayıtları tutulmaktadır.
2. Tutulma kararı hakkını yönetim saklı tutar.

3.6. Gizlilik ve İfşa etmeme Anlaşmaları Çerçevesi

1. Bilgi gizliliğinin, kurum ile üçüncü taraflar ve yükleniciler arasında sağlanması için gizlilik sözleşmeleri imza altına alınır.
2. Sözleşme şartları hukuk müşavirliği tarafından değerlendirilir.
3. Kapsam dâhilindeki personelle ilgili gizlilik ve ifşa etmeme şartları Disiplin Süreci ve 4857 sayılı İş Kanunu hükümlerine tabidir.

Doküman Kod	IKU-BSTDB-BTP-001	Revizyon Tarihi	
Yayın Tarihi	24.01.2022	Revizyon No	BTP-001-1.0

4. Yükleniciler ve 3.taraf hizmet sağlayıcılar ile imzalanan sözleşmeler, Hukuk müşavirliği tarafından kontrol edilir, imzalı sözleşmeler ilgili birim tarafından saklanır.

3.7. E-fatura Uygulaması

1. Gelir İdaresi Başkanlığı ile karşılıklı IP kısıtlaması mevcuttur.
2. SSL güvenli REST servisi ile iletişim kurulmaktadır.
3. Toplu imzalama için HSM cihazı mevcuttur.

3.8. Kayıtlı Elektronik Posta / Elektronik Tebligat Uygulaması

Elektronik Belge Yönetim Sistemi (EBYS) hizmeti Genel Sekreterlik tarafından verilmektedir.

1. Elektronik Belge ve Arşiv Yönetim Sistemi temel erişim yöntemleri olan “Kullanıcı İsmi” ve “Şifre” temelinde çalışmaktadır.
2. Elektronik Belge ve Arşiv Yönetim Sistemi’ ne kullanıcı ismi ve şifrenin yanı sıra Güvenlik Kodu Doğrulama ile de giriş yapılabilmektedir.
3. Sistem güvenliğini sağlamak amacıyla, sisteme hatalı giriş yapılan bağlantıları (IP) belirlemek ve şüpheli olanların girişini engellemek için kullanılır. Sadece Sistem Yöneticisi yetkisindeki kullanıcıların erişimine açıktır.
4. KEP, Genel Sekreterlik sorumluluğunda yönetilen hizmet olarak sağlanmaktadır. Anahtar yönetimi firma tarafından yapılmaktadır.

3.9. Web servisleri üzerinden bilgi paylaşma uygulaması

BŞT hizmetlerini içeren web servis geliştirmeleri Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı Yazılım Geliştirme ve İnovasyon birimi tarafından yapılmaktadır.

1. Web servisleri Rest mimarisi ile geliştirilmektedir.
2. Web servis giriş ve yetkilendirme OAuth2 protokolü ile gerçekleştirilmektedir.
3. Web servis domain adresleri SSL üzerinden hizmet vermektedir.
4. Web servis ile iletişim kuracak yazılımlar IP kısıtlamasına tabi tutulurlar.

Üniversitemizin, kaynaklarının planlanmasını ve yönetilmesini sağlayan sistemin merkezi programı SAP yazılımıdır. Yazılımın idaresini Kurumsal Bilgi Yönetim Daire Başkanlığı yürütmektedir.

Kurumun merkezi yönetim yazılımı olması nedeni ile kurum içi ve kurum dışı paydaşlara veri paylaşımı yapılmaktadır.

Kurum dışı veri paylaşımı;

1. Kurum dışı paydaşlar ile karşılıklı IP kısıtlaması yapılmaktadır.
2. SSL destekli REST ile WEB servisi olmak üzere iki bağlantı türü kurulmaktadır.

Doküman Kod	IKU-BSTDB-BTP-001	Revizyon Tarihi	
Yayın Tarihi	24.01.2022	Revizyon No	BTP-001-1.0

3. Servisler kimlik doğrulaması ile çalışmaktadır.

Kurum içi veri paylaşımı;

1. Kurum içi veri paylaşimleri Rest, Web Servis ve en büyük paylaşım MSSQL sunucusu üzerinden üç bağlantı türü bulunmaktadır.
2. Servislere erişim kimlik doğrulaması ile yapılmaktadır.
3. Servislere yerel ağ dışından erişim yapılamaz.

4. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar

Doküman Kod	IKU-BSTDB-BTP-001	Revizyon Tarihi	
Yayın Tarihi	24.01.2022	Revizyon No	BTP-001-1.0