İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

BİLGİ GÜVENLİĞİ OLAY İHLAL PROSEDÜRÜ

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

İÇİNDEKİLER

1. AMAÇ

Bu prosedür, bir Bilgi Güvenliği (BG) olayı/ihlali/açıklığı durumunda, olayın/ihlalin/açıklığın incelenmesi ve değerlendirilmesi için yapılacak olan işlemleri, ilgili kişilerin görev ve sorumluluklarını ve hazırlanacak olan formları tanımlamak amacıyla hazırlanmıştır.

2. KAPSAM

Bu prosedür, tüm İstanbul Kültür Üniversitesi birimleri dahilinde meydana gelen BG olayı/ihlali/açıklıkları konularının incelenmesi ve değerlendirilmesi durumunu kapsamaktadır.

3. SORUMLULAR

SORUMLULAR	TANIMLAR
BGYS Yönetim Temsilcisi:	Sistemin işletilmesinden sorumludur. Tüm olay / açıklık bildirimlerinden 1. Derecede sorumludur.
Diğer:	İlgili paragraf, bölüm, sorumluluk veya talimatın altında belirlenmiştir.

4. İLGİLİ DOKÜMANLAR

İlgili paragraf, bölüm, sorumluluk veya talimatın altında belirlenmiştir.

5. TANIMLAR VE KISALTMALAR

SORUMLULAR	TANIMLAR
DEĞERLİ VARLIK:	Gizlilik, bütünlük ve erişilebilirlik özelliklerinden birisinin etkilenmesi durumunda kurumu etkileyebilecek potansiyeli olan bütün kurum varlıklarıdır.
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS):	İstanbul Kültür Üniversitesi için değerli bilgi varlıklarının üretildiği, saklandığı, işlendiği bilgiler ve bilgi işleme araçlarından oluşan bütündür.
BİLGİ GÜVENLİĞİ OLAYI:	İstanbul Kültür Üniversitesinin değerli bilgi varlığının/varlıklarının gizliliği, bütünlüğü, erişilebilirliği değerlerinden bir veya birkaçının kuralsız bir şekilde bozulmasına sebep olan olaydır. Her BG olayı BG ihlali olarak değerlendirilmeyebilir.
BİLGİ GÜVENLİĞİ İHLALİ:	İstanbul Kültür Üniversitesinin BG kapsamındaki değerli varlıklarını korumaya yönelik ilgili politika, prosedür, talimatların, uyulması zorunlu olan ilgili kanun ve yönergelerin dışına çıkan bilinçli / bilinçsiz olarak gerçekleştirilen her türlü ihlaldir. Her BG ihlali aynı zamanda BG olayıdır.

BİLGİ GÜVENLİĞİ AÇIKLIĞI:	İstanbul Kültür Üniversitesine ait bilgi varlıklarının korunmasızlıklarıdır. Açıklık potansiyel tehditler tarafından kullanılan zayıflıklardır.

6. YÖNTEM

6.1. Bildirim Şartları

Bilgi güvenliği ile ilgili her tür olay, açıklık derhal gören, yaşayan tarafından BG Koordinatörüne bildirilir. Her bildirim kayıt altına alınır. BG Koordinatörüne her durumda e posta bildirimi yapılır ve daha sonra "**Olay Halinde İletişime Geçilecek Birim / Kişi Tablosu**ndaki birimlere / kişilere yazılı, sözlü ve herhangi bir iletişim aracı ile rapor edilir.

6.2. Bilgi Güvenliği Sorumlulukları ve prosedürleri

Bilgi güvenliği olaylarının yönetilmesi Bilgi Güvenliği Koordinatörünün sorumluluğundadır.

Tüm personel bilgi güvenliği ihlallerini ve zayıflıklarını farkına vardıkları zaman hemen Bilgi Güvenliği Yöneticisine rapor edeceklerdir. İhlal, çalışan bazlı ve kurumsal kayıplara yol açmış ise "Disiplin Prosedürü" çerçevesinde süreç işletilecektir.

Tedarikçi bazlı ise gizlilik sözleşmesi hükümlerine göre işlem başlatılacaktır.

Müşteri bazlı ise iş ve gizlilik sözleşmelerindeki hükümler değerlendirilecektir.

Hukuki süreçlerin işletilmesi kararı Rektörlüğe aittir.

Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları oluşturulmuş, yayınlanmış ve taraflara bildirilmiştir. Bu nedenle aşağıdaki yapı kurulmuştur:

Bilgi Güvenliği Olay Değerlendirme Kurulu: Önemli / büyük bir BG olayı veya kırılması durumunda derhal veya düzenli gözden geçirme toplantılarında BG olaylarını incelemek ve bir sonuca ulaştırmaktan sorumludur.

Bilgi Güvenliği Yöneticisi: Tüm kurumun en tepedeki BG icra sorumlusudur. Bir BG olayı meydana geldiğinde, olayın ilk değerlendirmesini yapacak, derhal müdahale ve tedbiri gerektiren bir olay ise Bilgi Güvenliği Olay Müdahale Ekibini görevlendirerek olaya süratle müdahale edilmesini sağlayacaktır. Olay yerinin ve olaya ilişkin kanıt ve verilerin korunmasından sorumludur.

Bilgi Güvenliği Sorumlusu: Dağıtık yapılarda koordinatöre bağlı çalışan birim bilgi güvenliği yöneticisidir.

Bilgi Güvenliği Olay Müdahale Ekibi: Bildirilen olayın niteliğine göre oluşturulmuştur. Bildirilen olaylara müdahale etmek, olay etkilerini azaltmak veya olay tehditlerinden sistemleri izole etmek / zayıflıklarını yönetmek üzere görevlendirilmiş geçici ekiptir. Her türlü kanıt, belge ve bulguları elde ederek bilgi güvenliği olaylarının aydınlatılmasını sağlamaktan sorumludur.

İlgili Dokümanlar:

- Müdahale Sorumlulukları ve Talimatları
- IKU BGYS Roller ve Sorumluluklar Dokümanı
- Yükseköğretim Kurumları Yönetici, Öğretim Elemanı ve Memurları Disiplin Yönetmeliği

6.3. Bilgi Güvenliği Olaylarının Bildirimi

İstanbul Kültür Üniversitesi politika ve talimatlarına uymayan her tür davranış, İstanbul Kültür Üniversitesi bilgi güvenliği prensipleri, politika ve talimatlarına aykırı her tür bilgi paylaşımı, uygunsuz bilgisayar kullanımı, yetkisiz girişler, dış / iç kaynaklı olarak yapılan ataklar, uygun olmayan yerde yetkisiz personelin görülmesi, bilgi varlıkları ile ilgili arızalar, kesintiler, hırsızlık, kaybolmalar, deprem, sel, su basması, yangın felaketler, toplumsal olaylar, savaş durumları gibi mücbir sebepler, bilgi güvenliği olayı kapsamına girmektedir.

1. Fiziksel olaylar / felaket hallerinde müdahaleyi ilgili acil durum ekipleri yaparlar.
2. Bilişim sistemleri üzerinde bildirilmiş olaylar, eğer raporlayan personelin rol ve sorumluluklarına girmiyorsa raporlayan kişinin olaya müdahale etmemesi, hiçbir şeye dokunmaması gerekmektedir. Gerekli iş ve işlemleri konunun uzmanları tarafından başlatılacaktır.

   Eğer olayı raporlayan personelin olaya müdahale etmesi konusunda görev ve sorumluluğu mevcut ise;

   2.1. ***Adli bilişim konusunda:*** Gerekli bildirimlerden sonra olay kanıtlarını yok etmeyecek veya delil karartmaya mahal vermeyecek şekilde olay etrafını izole eder ve delil toplama konusundaki uzmanın çalışması için çevresel şartları oluşturur.

   2.2. ***Adli bilişim dışında:*** Olaya müdahale eder. Olayı kontrol altına aldıktan sonra gerekli bildirimleri yapar.

6.4. Bilgi Güvenliği Açıklık / Zayıflıklarının Bildirimi

Bilgi güvenliği ile ilgili olarak tespit edilen bir açıklık, derhal gören, yaşayan tarafından BG Olay Yöneticisine veya "**Olay Halinde İletişime Geçilecek Birim / Kişi Tablosu**"ndaki birimlere / kişilere yazılı, sözlü veya herhangi bir iletişim aracı ile rapor edilmelidir.

İlgili Doküman:

- Risk Analizi | Açıklık Tablosu
- İhlal Olay Halinde İletişime Geçilecek Birim / Kişi Tablosu
- İhlal Olay Bildirim Formu

6.5. Bilgi Güvenliği Olaylarında Değerlendirme ve Karar Verme

Bilgi güvenliği olaylarının değerlendirilmesi, sınıflandırılması ve müdahale / çözüm süreçlerinin yönetilmesi Bilgi Güvenliği Koordinatörü görevleri içindedir.

Kurumda bilgi güvenliği olayları ve zayıflıkları için bildirim formu hazırlanmıştır. BG Koordinatörü formun gelmesi veya güvenlik olayının kendisine sözlü olarak bildirilmesine bağlı olarak derhal olay inceleme ve değerlendirmesi yapar. Önlemler / çözümler için tepki kararını verir.

Sonuçları Olay /zayıflık bildirim formuna işler. Sözlü gelen bildirimlerin daha sonra kayıt altına alınmasını sağlar.

İlgili Doküman:

- İhlal Olay Halinde İletişime Geçilecek Birim / Kişi Tablosu
- İhlal Olay Bildirim Formu

6.6. Bilgi Güvenliği İhlal Olaylarına Yanıt Verme

Ortaya çıkan bir güvenlik olayı veya kırılmasına dair değerlendirme Bilgi Güvenliği Koordinatörü tarafından yapılır. Bilgi Güvenliği Koordinatörünün kararı ile olaya müdahale edilir.

Müdahale işlemleri ve olayın sonuçlarının kontrol altına alınması Bilgi Güvenliği Olay Müdahale Ekibindedir. Bilgi Güvenliği Olay Müdahale Ekibi gerekli çalışmalardan sonra sonuçları Bilgi Güvenliği Koordinatörüne raporlar.

Bilgi Güvenliği olayının hukuki, cezai takibi veya yaptırımları söz konusu ise veya kurumsal açıdan önem arz ediyorsa Bilgi Güvenliği Yönetim temsilcisi Olay / açıklık sonuç raporu hazırlar ve yönetime sunar.

İlgili Doküman:

- İhlal Olay Halinde İletişime Geçilecek Birim / Kişi Tablosu
- İhlal Olay İnceleme Raporu

6.7. Bilgi Güvenliği İhlal Olayından Öğrenme

İhlal olayları ve açıklıklar "Bilgi Güvenliği Olayları Durum Raporu"na kaydedilir. 6 ayda en az bir kez değerlendirilerek eğilimler belirlenir.

Değerlendirmeler Bilgi Güvenliği Olayı Değerlendirme Kurulunda yapılır.

Kurulun değerlendirmeleri ve kararları risk değerlendirme çalışmalarında ve Yönetimin Gözden Geçirilmesi toplantılarında girdi olarak kullanılır.

İç tetkik esnasında bulgulanan ihlal veya açıklıklar iç tetkik raporuna aktarılır.

Alınması gereken önlemler varsa risk değerlendirmesine bağlı olarak YGG toplantısında gözden geçirilir.

İlgili Doküman:

- İhlal Olay İnceleme Raporu
- İhlal Olay Durum Dönem Raporu

6.8. Kanıt Toplama

Bilgi güvenlik olayının ardından kişi ya da kurumlara karşı takip uygulama gerekmesi hali düşünülerek herhangi bir suç isnadı olmasa bile deliller mutlaka toplanır ve uygun şekilde muhafaza edilir.

Bilgi Güvenliği Yöneticisi kendisine bildirimi yapılan ihlal ve zayıflığı görmek, incelemek ve gerekli delilleri toplamak amacı ile olay mahallini veya olayın vuku bulduğu bilgi varlıklarını görür, gerektiğinde fotoğraf veya kamera ile kayıt altına alır, gerekli kişilerle konuşur ve bulgularını raporlar.

Eğer delil toplama araçları / yöntemleri yoksa adli kolluk gelinceye dek ortamın güvenliği sağlanır.

İlgili Doküman:

- İhlal Olay İnceleme Raporu
- Adli Bilişim Delil Toplama Araç Yöntem Rehberi

7. MÜDAHALE SORUMLULUKLARI ve TALİMATLARI

7.1. Bilgi Sistemleri Hataları ve Hizmet Kayıpları Durumunda

Sorumlular: Sistem ve Ağ Yöneticileri

Yöntem: Yerel ağ hizmetleri için önce sorunun kaynağı araştırılır. Durum günlüklerine (event log) bakılır. Firewall ve router günlükleri incelenerek saldırı durumları değerlendirilir. Kablo ve cihazlar fiziksel olarak kontrol edilir.

İlgili Doküman:

- Sunucu Güvenliği Talimatı
- Sunucu Bakım Kontrol Listesi
- Veri tabanı Kontrol Formu
- Adli Bilişim Delil Toplama Araç ve Yöntemleri Rehberi

7.2. Taşınır veya Taşınmaz Bilgisayarlar ve Fiziksel Sunucular İçin

Sorumlular: Sistem, Destek ve Ağ Yöneticileri

Yöntem:

a) Virüs, worm, trojan, tanımsız program bulunması durumunda

Öncelikle bilgisayar ağdan çıkarılır, sistem güvenli modda başlatılır ve virüs bulaştığı bildirilen klasör temizlenir. Ardından malware taraması yapılır. Yetkisiz tüm programlar silinir ve tüm virüsler temizlenir.

b) Herhangi bir BT hizmetinin durması durumunda

- Hizmet sunucularla ilgili ise problem sunucuların bakımını yapan personele haber verilir.
- Hizmet, telefonla ilgili ise santralin bakımını yapan personele haber verilir.
- Hizmet internet ile ilgili ise modemler ve Metro Ethernet devreleri kontrol edilir. Sorun kullanıcıdan kaynaklanıyorsa AD / LDAP' üzerinden kullanıcı konfigürasyonuna bakılır.

Bilgisayarın çalışamaz hale gelmesi durumunda ve işletim sistemi problemlerinde sistem geri yükleme opsiyonu ile sistem önceki haline getirilmeye çalışılır. Geri getirilemeyen sistemler için sistemdeki önemli bilgilerin bulunduğu klasörlerdeki veriler yedeklenerek sistem formatlanır.

İlgili Doküman:

- IKU BSTDB Yedekleme Prosedürü
- IKU BSTDB Varlıkların Kabul Edilebilir Kullanımı Politikası içinde (Antivirus Yazılımı Kullanım Talimatı)

7.3. Veri Kaybı Durumunda

Sorumlular: Sistem ve Ağ Yöneticileri

Yöntem:

- Kaybolan verinin yedekleri olup olmadığına bakılır.
- Yedekler varsa yedeklerden geri dönüş yapılır.
- Yedekler yoksa veya geri dönüş noktası kaybolan bilginin özelliğine göre eski kalıyorsa recovery işlemleri yapan araçlarla silinen verilerin geri alınması çalışması başlatılır.
- Yanma, kırılma ve benzeri fiziksel hasarlarda kritik veri kayıpları için veri kurtarma hizmeti veren kurumlarla iletime geçilir.

İlgili Doküman:

- IKU BSTDB Yedekleme Prosedürü

7.4. Gizlilik, Politika ve Talimatlara Aykırı Hareketler

Sorumlular: Bilgi Güvenliği Koordinatörü

Yöntem: İdare personelinin, 3. Taraf hizmet veren / yüklenici firma çalışanlarının İstanbul Kültür Üniversitesine ait bilgilerin gizliliğine ve İstanbul Kültür Üniversitesi bilgi güvenliği politika ve talimatlarına aykırı hareket etmesi durumunda "Olay İhlal ve Açıklık Formu" doldurulur ve Bilgi Güvenliği Koordinatörü'ne haber verilir. Rektör'ün onayı ile Bilgi Güvenliği Koordinatörü olay ile ilgili "Disiplin Prosedürü"nü hayata geçirir.

İlgili Dokümantasyon:

- Yükseköğretim Kurumları Yönetici, Öğretim Elemanı ve Memurları Disiplin Yönetmeliği
- IKU BSTDB Varlıkların Kabul Edilebilir Kullanımı Politikası

7.5. Bilgi Sistemlerinin Uygunsuz Kullanımı

Sorumlular: Bilgi Sistemleri ve Teknolojileri Daire başkanı, Sistem ve Ağ Yöneticileri ve Bilgi Güvenliği Koordinatörü

Yöntem: Bilgi sistemlerine içeriden sızmaya çalışan, açıklıkları tespit edip bu açıklıkları kullanmaya çalışan İdare personelinin, 3. Taraf hizmet veren / yüklenici firma çalışanlarının tespiti halinde "Olay İhlal ve Açıklık Formu" doldurulur ve Bilgi Güvenliği Koordinatörü'ne haber verilir. Rektör'ün onayı ile Bilgi Güvenliği Koordinatörü olay ile ilgili "Disiplin Prosedürü"nü hayata geçirir.

Bilgi güvenlik olayının ardından kişi ya da kurumlara karşı takip uygulama gerekmesi hali düşünülerek herhangi bir suç isnadı olmasa bile deliller mutlaka toplanır ve uygun şekilde muhafaza edilir. Bilgi Güvenliği Koordinatörü, bildirimi yapılan ihlal ve zayıflığı görmek, incelemek ve gerekli delilleri toplamak amacı ile olay mahallini veya olayın vuku bulduğu bilgi varlıklarını görür, gerektiğinde fotoğraf veya kamera ile kayıt altına alır, gerekli kişilerle konuşur ve bulgularını raporlar.

İdarenin tespit edilen olayı adli mercilere bildirmesi gerekiyorsa, ilgili sistem yöneticileri veya idareciler olay kanıtlarının yok edilmesine veya delillerin karartılmasına mahal vermeyecek şekilde olayın etrafını izole eder ve delil toplama konusundaki uzmanın çalışması için çevresel şartları oluşturur.

İlgili Dokümanlar:

- Adli Bilişim Delil Toplama Araç ve Yöntemleri Rehberi
- IKU BSTDB Varlıkların Kabul Edilebilir Kullanımı Politikası

8. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar
