REVİZYON TABLOSU

REVİZYON NO	REVİZYON GEREKÇESİ	TARİH
01	2022 versiyon değişikliği	01.10.2024

1. AMAÇ

Bu prosedür; Aksaray Üniversitesi bilgi güvenliği ihlal olaylarının yönetimine, güvenlik olayları ve açıklıklar üzerindeki bağlantısını da içeren, tutarlı ve etkili bir yaklaşımın uygulanmasını sağlayacak yöntem ve kuralları anlatmak düzenlenmiştir.

2. KAPSAM

Bu prosedür; Bilgi Güvenliği Yönetim Sistemi kapsamında güvenlik ihlal olaylarının yönetimi için alınacak tedbirleri ve bu tedbirlerin uygulanmasına ait yönetimi kapsar.

3 UYGULAMA

3.1 BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

3.1.1 Bilgi Güvenliği İhlal Olaylarının ve İyileştirmelerin Yönetimi

3.1.1.1 Sorumluluklar ve Prosedürler

Bilgi güvenliği ihlal olayları ile ilgili otoriteler, dış ilgi grupları ya da forumlarla, ihlal olaylarınıele alacak yetkili personel, dâhili ve harici kişi ya da kuruluşlara ait iletişim listesi BGYS/BF/001 İlgili Taraf Beklentiler ve İletişim Formunda tanımlanmış gerekli durumlarda iletişim sağlanmaktadır.

Bilgi güvenliği olaylarının ve ihlal olaylarının izlenmesi, tespiti, analizi ve raporlanması, İhlal olayları yönetimi faaliyetlerine ait kayıtların tutulması, adli delil işlenmesi, bilgi güvenliği olaylarının değerlendirilmesi, bilgi güvenliği olaylarında karar verme, Bilgi güvenliği ihlal olaylarını ele alacak yetkili personel ve Güvenlik ihlallerini işleyen çalışanlar ile ilgili işlemleriçin yürütülecek disiplin proseslerine ait yöntem ve kurallar **3.1.1.2, 3.1.1.3, 3.1.1.4, 3.1.1.5, 3.1.1.6 ve 3.1.1.7** maddelerinde ele alınmıştır.

3.1.1.2 Bilgi Güvenliği Olaylarının ve Açıklıklarının Raporlanması

- ✓ Kurum ve tedarikçi çalışanları herhangi bir Bilgi Güvenliği olayını, sistemlerde veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığını tespit ettiklerinde, vakit kaybetmeden mümkünse öncesinde BGYS/BF/007 Bilgi Güvenliği İhlal Olayı Formunu doldurarak mümkün değilse diğer iletişim kanallarını kullanarak (Telefon, E-mail) BGYS Yöneticisine ve/veya ilgili bölüm yöneticilerine bildirmekle yükümlüdürler.
- ✓ Tüm çalışanlar ve yükleniciler, herhangi bir güvenlik olayını olabildiğince hızlı bir şekilde kurumumuz tarafından belirlenen iletişim noktalarına raporlanması ile bilgilendirilmiştir.

✓ Bilgi güvenliği olaylarına ve açıklıklarına yönelik ön sınıflandırma tanımları aşağıda açıklanmıştır;

Bilgi Güvenliği Olayları

- Etkisiz güvenlik kontrolü,
- Bilginin bütünlük, gizlilik veya erişilebilirlik beklentilerinin ihlali,
- İnsan hataları, (Kullanıcı hataları)
- Talimatlar ve kılavuzlarla uygunsuzluk, (Şifre kuralları, şifre kullanımı, Varlıkların kabul edilebilir kullanım kuralları, İnternet kullanım kuralları, E-Posta kullanım kuralları ve ilgili diğer BGYS talimatlarına aykırı hareket etme, talimatlara aykırı bilgi transferi, Temiz masa ve Temiz ekran politikası ihlali)
- Fiziksel güvenlik düzenlemelerinin ihlali,
- Kontrolsüz sistem değişiklikleri,
- Yazılım ya da donanım arızaları,
- Erişim ihlalleri (Yetkisiz erişimler)

Bilgi Güvenliği Açıklıkları

- Zararlı yazılım (Virüs) tespiti,
- Yazılım açıklıkları,
- Bilgi Teknolojileri ile ilgili Hizmetlerin kesilmesi, Durması
- Siber Saldırı / Casusluk
- Bilginin çalınması

✓ Güvenlik ihlaline neden olan ve olaya tanık olan ve bildirmeyen firma ve tedarikçi çalışanları,üçüncü taraflar hakkında BGYS/BT/01Disiplin Talimatına göre resmi bir disiplin süreci uygulanır.

3.1.1.3 Bilgi Güvenliği Olaylarında Değerlendirme ve Karar Verme

Firma ve tedarikçi çalışanları ile üçüncü taraflara ait bilgi güvenliği olayları ve/veya açıklıklarına ait yapılan bildirimler Acil Müdahale Ekibi Başkanı ve BGYS Yöneticisi tarafından olayın bir bilgi güvenliği ihlal olayı olarak sınıflandırılıp sınıflandırılamayacağı ile ilgili olarak değerlendirilir. Değerlendirme aşamasında ihtiyaç duyulduğu takdirde gerekliteknik uzmanlık ve diğer hususlar için diğer birim yöneticilerinden yardım ve destek alınır.

✓ Olayın boyutlarının kurumumuz süreçlerine etkisi BGYS/BF/007 Bilgi Güvenliği İhlal Olayı

Formunda yer alan Değerlendirme Matrisi ile tespit edilir.

- ✓ Değerlendirme sonuçları BGYS yöneticisi tarafından bilgi güvenliği kuruluna gönderilir. Bilgi güvenliği kurulu olayla ilgili değerlendirme sonuçlarına ve olayın tanıklarından aldıkları bilgilere göre Firma çalışanları, tedarikçi ve/veya tedarikçi çalışanları hakkında herhangi bir disiplin veya cezai yaptırım uygulanıp uygulanmayacağına ve/veya hukuki/resmi bir işlem başlatılıp başlatılmayacağına karar verir ve bilgi güvenliği disiplin talimatına ve/veya gizlilik sözleşmeleri esaslarına göre resmi bir disiplin sürecini uygulanır.
- ✓ Bilgi güvenliği olaylarına ve açıklıklarına ait kayıtlar ileride tekrar faydalanma ve doğrulama amacıyla saklanmaktadır.

3.1.1.4 Bilgi Güvenliği İhlal Olaylarına Müdahale

- ✓ Bilgi güvenliği ihlal olaylarına müdahale Acil Müdahale Ekibi Başkanı ve BGYS Yöneticisi tarafından olayın niteliği, etkisi, ve toplanan deliller çerçevesinde yönlendirmesi ile acil müdahale ekibi üyeleri tarafından ve/veya dış taraflarca kendilerine atanan, istenen görevler çerçevesinde ihlal olayını gerçekleştiren veya buna katkıda bulunan bilgi güvenliği zayıflığı/zayıflıkları ve açıklıklarını da ele alınarak olayın, açıklığın kapatılmasına ve bir daha tekrarlanmamasına yönelik olarak planlanır ve gerçekleştirilir. Gerektiği durumlarda bilgi güvenliği adli bilişim analizi yapılması sağlanır.
- ✓ Acil müdahale ekibi üyeleri tarafından ve/veya dış taraflarca yapılan müdahaleler sonunda gerçekleştirilen faaliyetler Acil Müdahale Ekibi Başkanı ve BGYS Yöneticisi tarafından incelendikten sonra yeterli bulunursa ihlal olayı kaydı kapatılır. Yeterli görülmediği takdirde ilave faaliyetler ile ilgili yeni görevlendirmeler Acil Müdahale Ekibi Başkanı ve BGYS Yöneticisi tarafından faaliyetin kapatılmasına yönelik planlanabilir.
- ✓ İhlal olaylarının müdahale faaliyetlerine yönelik kayıtlar, kanıtlar korunarak saklanmaktadır.
- ✓ Bilgi güvenliği ihlal olaylarına ait detay bilgilerin Bilmesi Gereken Prensibine göre kurum içi ve dışı kişi veya birimlere duyurulması sağlanır.

3.1.1.5 Bilgi Güvenliği İhlal Olaylarından Ders Çıkarma

- ✓ Bilgi güvenliği ihlal olaylarının analizi ve çözümlemesinden kazanılan bilgi birikimi gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için kullanılmaktadır.
- ✓ Bilgi güvenliği ihlal olaylarına ait değerlendirme ve aksiyon kayıtları (bilgi güvenliği ihlal olayı bildirim formları, değerlendirme matrisleri ve aksiyon kayıtları) tekrarlanan yada yüksek etkili ihlal olaylarını tespit etmek için kullanılmakta ve kayıtlar saklanmaktadır.
- ✓ Gerekiyor ise ilave kontroller devreye alınır.

3.1.1.6 Kanıt Toplama

Bilgi güvenliği ihlal olaylarında kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunması için aşağıdaki yöntemler dikkate alınır;

- ✓ Genel olarak bilgi güvenliği ihlal olayı kanıtları ile ilgili ortam ve aygıtların farklı türleri ve cihazların durumu (örneğin; cihazın açık veya kapalı olması) ile uyumlu kanıt tespiti, toplama, edinim ve korunmasına yönelik aşağıdaki hususlar dikkate alınır.
  - **a)** Delil zinciri,
  - **b)** Kanıt emniyeti,
  - **c)** Personel emniyeti,
  - **d)** İlgili personellerin rolleri ve sorumlulukları,
  - **e)** Personel yeterliliği,
  - **f)** Dokümantasyon,
  - **g)** Bilgilendirme.

- ✓ Bilgi güvenliği olayı ilk tespit edildiğinde, bu olayın hukuki/yasal bir süreç başlatılmasına neden olup olmayacağının açıkça anlaşılana kadar toplanan kanıtlar kasıtlı ya da kazayla imha edilmesi tehlikesine karşı Bilgi Güvenliği Acil Müdahale Ekibi tarafından korunur.
- ✓ Bilgi güvenliği Acil Müdahale Ekibinde görev alacak ve bilgi güvenliği ihlal olayına müdahaleedecek personellerin uygun olduğu durumlarda yeterli niteliklere sahip olması ile ilgili gerekli eğitimlerin alınması sağlanır. (olay kanıtlarının toplanması ve korunması, olaylara müdahale, olayların ve açıklıkların kapatılması vb.)
- ✓ Adli vaka olarak tespit edilen İhlal olayları üst yönetim onayı ile uygun iletişim kanalları kullanılarak avukat ve polise bildirilir.
- ✓ Adli olaylarda toplanan kanıtların değerinin güçlendirilmesine yönelik olarak, mümkünse ilgili kurumun sertifikasyon ya da diğer personel nitelikleri ile ilgili yöntemlerin ve araçların kullanılması sağlanır.

4. SORUMLULUK

Kapsam dâhilindeki tüm personel Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü uygulama esaslarına uygun hareket etmekle yükümlüdür.

5. EK

BGYS/BF/001 İlgili Taraf Beklentiler ve İletişim Formu

BGYS/BF/007 Bilgi Güvenliği İhlal Olayı Formu

BGYS/BT/01Disiplin Talimatı