1. **AMAÇ:** Fakültemiz kapsamı dâhilinde yaşanabilecek bilgi güvenliği ihlalleri noktasında durumun nasıl yönetileceğini ifade eder.

2. **KAPSAM:** Fakültemizin tüm birimlerini kapsar.

3. **KISALTMALAR:**

4. **TANIMLAR:**

Trojan: Trojanlar tüm kişisel belgelerimizi saniyeler içerisinde kopyalanabilen oldukça tehlikeli yazılımlardır. Trojan bulaşan bir bilgisayara her an uzaktan erişilebilir. Trojanlar, Truva atı olarakta bilinmektedir.

Spyware: Spyware veya Türkçe ismi ile casus programlar bilgisayarınızda casusluk yapmak için yaratılmış programlardır. Bu programlar kullandığınız masum görünen ve genelde internetten "bedava" diye reklâmını görüp indirdiğiniz programlar ile bilgisayarınıza bulaşan programcıklardır.

5. **SORUMLULAR:** Fakültemizde bilgisayar kullanan tüm personeli

6. **FAALİYET AKIŞI:**

Bilgi Güvenliği İhlal Olayları, Fakültemiz kapsamında aşağıdaki gibi yönetilmektedir.

- Fakültemiz Bilgi Güvenliği Politikası ve Prosedürlerine uymayan kişiler ve aykırı her tür davranış,
- Veri kaybı, bilgilere yetkisiz kişilerin erişimi,
- Virüs, izinsiz giriş, trojan, spyware vb. bulgular,
- Uygunsuz PC/Laptop kullanımı, , uygun olmayan yerde yetkisiz personelin görülmesi,
- Bilgisayar varlıkları ile ilgili hırsızlık, kaybolma, yanma, kırılma vb. olumsuzluklar,
- Donanım arızaları, network, sistem, sunucu, servis problemleri,
- Ağ üzerinden saldırı,
- Her türlü bilgi güvenliği ihlal olayları

Yukarıda bahsedilen bilgi güvenliği ile ilgili ihlal olaylarında Fakültemiz Bilgi Güvenliği Yetkilileri derhal haberdar edilmelidir. Olay halinde müdahaleyi ilgili/yetkili birimler yaparlar. Olayı raporlayan kişinin müdahale etmemesi ve uzmanların müdahalesi için hiçbir şeye dokunmaması gerekmektedir.

Zayıflıkların (politikaya direnen kullanıcılar, işletim sistemindeki eksik yamalar, e-postalardaki spamın artması, sistemin yavaşlaması, cihazların fazla ısınması, giriş ve çıkışlarda tespit edilen yetkisiz girişe uygun alanlar ve durumlar, kapatılmayan kapılar kilitlenmeyen dolaplar, kapatılmayan oturumlar (bilgisayarı açık bırakıp gitme), dağınık ve halka açık ortamlarda duran bilgiler vb. gibi gözlenen olaylar) tespiti durumunda önlem alınması için kişinin sözlü veya yazılı olarak bildirimi gereklidir. Olası bir tehdide meydan verecek bir zayıflığı tespit eden çalışanlar "zayıflığı test etmeden" derhal aşağıdaki yetkililere haber vermelidirler.

OLAY TANIMI	**YETKİLİ KİŞİ/KURUM**	**İLETİŞİM BİLGİLERİ**
Her türlü bilgi güvenliği ihlal olayları durumunda	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544
Virüs, izinsiz giriş, trojan, spyware vb. bulgular için, sistem sunucu servis problemleri için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544
Donanım arızaları, Network Problemleri için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544
Veri kaybı, bilgilere yetkisiz erişim Durumlarında	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544
Hırsızlık, kaybolma, yanma, kırılma vb. durumlar için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544
Uygunsuz davranışlar ve politikaya uymayan kişiler için	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544
Ağ üzerinden Saldırı	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544
Bilgisayarınızda Anti Virüs Programı yüklü değilse	E.Ü Diş Hekimliği Fakültesi Bilgi İşlem Birimi	Dahili: 4555 ve 1544

7. İLGİLİ DOKÜMANLAR:

Bilgi Yönetimi ve Güvenliği Prosedürü