1. AMAÇ

Süleyman Demirel Üniversitesi Entegre Yönetim Sistemi (EYS) kapsamına dahil olan birimlerin bünyesinde kullanılan resmi ve kişisel sosyal medya hesaplarının güvenli, kontrollü ve mevzuata uygun şekilde kullanılmasına ilişkin kuralları belirlemektir.

Bu politika ile sosyal medya platformlarının kullanımından kaynaklanabilecek;

- Bilgi güvenliği ihlallerinin,
- Yetkisiz bilgi ve belge paylaşımının,
- Kişisel veri ve özel nitelikli kişisel veri ihlallerinin,
- Hasta ve sağlık verilerinin yetkisiz şekilde paylaşılmasının,
- Sosyal mühendislik ve kimlik avı saldırılarının,
- Yetkisiz hesap erişimlerinin,
- Kurumsal itibar kaybının,
- Telif ve fikri mülkiyet hakkı ihlallerinin önlenmesi veya azaltılması amaçlanmaktadır.

2. KAPSAM

- Süleyman Demirel Üniversitesi Daire Başkanlıklarını,
- Genel Sekreterliği,
- Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimini,
- Bu birimlerde görev yapan akademik ve idari personel, işçiler, bilişim personeli, sözleşmeli personel, stajyerler ve görevleri kapsamında Üniversite bilgi varlıklarına erişen diğer kişileri,
- Üniversite ve bağlı birimler adına yönetilen resmi sosyal medya hesaplarını,
- Üniversite bilgi varlıkları, kişisel veriler veya kurumsal bilgilerle ilişkili kişisel sosyal medya kullanımını kapsar.

Üniversitenin resmi sosyal medya hesaplarının yanı sıra, kişisel sosyal medya hesaplarının kullanımında Üniversiteye ait bilgi ve bilgi varlıklarının korunması, kişisel verilerin korunması ve kurumsal bilgilerin yetkisiz paylaşılmaması bakımından uygulanır.

3. SORUMLULUKLAR

3.1. Tüm Personel ve Kullanıcılar

- Üniversiteye ait bilgi ve bilgi varlıklarını korumak,
- Yetkileri dışında Üniversite adına sosyal medya paylaşımı yapmamak,
- Gizlilik ve kritiklik değeri bulunan bilgileri sosyal medya platformlarında paylaşmamak,
- Kişisel verileri ve özel nitelikli kişisel verileri korumak,
- Sosyal mühendislik, kimlik avı ve sahte hesap girişimlerine karşı dikkatli olmak,
- Bilgi güvenliği veya kişisel veri ihlali şüphesi oluşturan durumları ilgili birimlere bildirmek,
- Bu politika ve ilgili EYS dokümanlarına uygun hareket etmek ile sorumludur.

3.2. Kurumsal İletişim Uygulama ve Araştırma Merkezi Müdürlüğü

Üniversitenin merkezi/resmi sosyal medya hesaplarının;

- Yönetilmesi,
- İçeriklerin koordinasyonu,
- Yetkili kullanıcıların belirlenmesi,
- Kurumsal iletişim açısından kontrol edilmesi,
- Paylaşımların izlenmesi faaliyetlerinden sorumludur.

3.3. Genel Sekreterlik

Genel Sekreterlik bünyesinde yürütülen resmi iletişim faaliyetleri kapsamında sosyal medya kullanımının ilgili mevzuat, Üniversite düzenlemeleri ve bu politika ile uyumlu yürütülmesini sağlar.

3.4. Daire Başkanlıkları

- Kendilerine ait veya kendi sorumluluklarında bulunan resmi sosyal medya hesaplarının yetkili kişilerce kullanılmasını,
- Yetkilendirilmiş kullanıcıların belirlenmesini,
- Görev değişikliği veya görevden ayrılma durumunda sosyal medya erişimlerinin gözden geçirilmesini,
- Birimlerine ait bilgi ve belgelerin yetkisiz şekilde sosyal medyada paylaşılmamasını sağlamakla sorumludur.

3.5. Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi

Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi;

- Hastane bilgi sistemlerine ilişkin teknik bilgilerin,
- Kullanıcı hesaplarının ve erişim bilgilerinin,
- Sistem yapılandırmalarının,
- Güvenlik açıklarının ve zafiyet bilgilerinin,
- Hasta ve sağlık verilerinin,
- Hastane bilgi işlem altyapısına ilişkin kritik bilgilerin sosyal medya veya yetkisiz platformlarda paylaşılmasını önlemeye yönelik gerekli kontrollerin uygulanmasından sorumludur.

Hastane Bilgi İşlem Birimi personeli, görevleri kapsamında eriştikleri hasta, çalışan veya diğer ilgili kişilere ait bilgileri kişisel veya resmi sosyal medya hesaplarında paylaşamaz.

3.6. Bilgi İşlem Daire Başkanlığı (BİDB)

- Sosyal medya kullanımından kaynaklanabilecek teknik bilgi güvenliği risklerinin değerlendirilmesine,
- Kurumsal hesapların teknik güvenlik kontrollerine,
- Kimlik doğrulama ve çok faktörlü kimlik doğrulama gibi güvenlik önlemlerine,
- Bilgi güvenliği olaylarının ilgili süreçlere aktarılmasına destek sağlar.

3.7. BGYS/KVYS Sorumluları

BGYS/KVYS kapsamında;

- Sosyal medya kullanımından kaynaklanan bilgi güvenliği ve kişisel veri risklerinin değerlendirilmesi,
- Gerekli kontrol ve iyileştirmelerin belirlenmesi,
- Tespit edilen olay ve uygunsuzlukların ilgili EYS süreçlerine aktarılması sağlanır.

4. TANIMLAR

SDÜ: Süleyman Demirel Üniversitesi

EYS: Entegre Yönetim Sistemi

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

KVYS: Kişisel Veri Yönetim Sistemi

KVKK: 6698 sayılı Kişisel Verilerin Korunması Kanunu

Resmi Sosyal Medya Hesabı: Üniversite veya Üniversiteye bağlı birimler adına yetkilendirilmiş kişiler tarafından yönetilen sosyal medya hesabı.

Kişisel Sosyal Medya Hesabı: Personel, öğrenci veya diğer kullanıcıların şahsi amaçlarla kullandıkları sosyal medya hesapları.

Sosyal Mühendislik: İnsanların güven, iletişim veya davranışlarından yararlanılarak bilgi veya erişim elde edilmesini amaçlayan yöntemler.

5. UYGULAMA

5.1. Genel Sosyal Medya Kullanım Kuralları

1. Sosyal medya kullanımında Üniversitenin bilgi güvenliği, kişisel verilerin korunması, kurumsal itibar ve ilgili mevzuat hükümleri dikkate alınır.
2. Üniversiteye ait bilgi ve bilgi varlıkları, yetkisiz kişi veya platformlarla paylaşılmaz.
3. Bilgi Sınıflandırma ve Etiketleme Politikası kapsamında sınıflandırılmış bilgilerin sosyal medya ortamında paylaşılması, ilgili yetki ve kurallar dışında gerçekleştirilemez.
4. Açık, Birime Özel, Hizmete Özel, Gizli ve Çok Gizli nitelikteki bilgilerin paylaşımı bilgi sınıflandırma kurallarına uygun şekilde gerçekleştirilir.
5. Özellikle aşağıdaki bilgiler sosyal medya ortamlarında paylaşılmaz:
    - Kullanıcı adı ve parolalar,
    - Kimlik doğrulama kodları,
    - Sistem erişim bilgileri,
    - IP adresleri ve teknik yapılandırma bilgileri,
    - Güvenlik cihazı yapılandırmaları,
    - Güvenlik açığı ve zafiyet bilgileri,
    - Sistem logları ve güvenlik kayıtları,
    - İç denetim ve güvenlik raporları,
    - Kurum içi yazışmalar,
    - Gizli veya kritik nitelikteki belgeler,
    - Yetkisiz kişilere ait kişisel veriler.
6. Üniversiteye ait bilgi ve belgeler kişisel sosyal medya hesapları üzerinden aktarılmaz.

5.2. Kişisel Verilerin Korunması

1. Sosyal medya paylaşımlarında 6698 sayılı KVKK ve Üniversitenin kişisel veri koruma düzenlemelerine uygun hareket edilir.
2. Kişisel veriler yalnızca gerekli hukuki şartların bulunması ve paylaşım amacının gerektirmesi halinde işlenir veya yayımlanır.
3. Sosyal medya paylaşımında gereğinden fazla kişisel veri kullanılmaz.
4. İsim, öğrenci numarası, personel bilgisi, telefon numarası, e-posta adresi, fotoğraf, video, sınav sonucu, başarı bilgisi ve benzeri kişisel veriler paylaşılmadan önce gerekli hukuki ve kurumsal kontroller yapılır.
5. Özel nitelikli kişisel veriler sosyal medya ortamında paylaşılmaz; özellikle sağlık verileri konusunda azami dikkat gösterilir.
6. Araştırma ve Uygulama Hastanesi kapsamında;
    - Hasta adı-soyadı,
    - Hasta numarası,
    - T.C. kimlik numarası,
    - Tanı ve tedavi bilgileri,
    - Tahlil ve görüntüleme sonuçları,
    - Reçete ve ilaç bilgileri,
    - Hasta fotoğrafı veya videosu,
    - Sağlık raporları,
    - Hastaya ilişkin diğer sağlık bilgileri yetkisiz sosyal medya paylaşımına konu edilemez.

7. Resmi sosyal medya hesaplarında kişisel veri içeren bir içeriğin yayımlanması gerektiğinde veri minimizasyonu uygulanır; gerekli hallerde kişisel veriler maskelenir veya anonim hale getirilir.
8. Fotoğraf ve video paylaşımlarında görüntüsü bulunan kişilerin kişisel verilerinin korunmasına ilişkin ilgili mevzuat ve Üniversitenin süreçleri dikkate alınır.

5.3. Resmi Sosyal Medya Hesaplarının Kullanımı

1. Üniversitenin ve birimlerin resmi sosyal medya hesapları yalnızca yetkilendirilmiş kişiler tarafından yönetilir.
2. Yetkisiz kişiler Üniversite adına resmi açıklama veya paylaşım yapamaz.
3. Resmi sosyal medya hesaplarının;
    - Kullanıcı adı,
    - Parolası,
    - Kurtarma bilgileri,
    - Doğrulama kodları,
    - Yönetici erişimleri yetkisiz kişilerle paylaşılmaz.

4. Destekleyen platformlarda çok faktörlü kimlik doğrulama kullanılması esastır.
5. Görev değişikliği veya görevden ayrılma durumunda ilgili kullanıcının sosyal medya hesabına erişim yetkisi gecikmeksizin gözden geçirilir ve gerekli durumlarda kaldırılır.
6. Resmi sosyal medya hesaplarında yayımlanacak içerikler, gerektiğinde ilgili birim yöneticisi ve Kurumsal İletişim Uygulama ve Araştırma Merkezi Müdürlüğü tarafından kontrol edilir.
7. Resmi hesaplarda gelen yorum, mesaj ve gönderilere cevap verilirken kurumsal iletişim ilkelerine uygun ve profesyonel bir dil kullanılır.
8. Mevzuata, Üniversite politikalarına veya kurumsal iletişim ilkelerine aykırı içeriklerin kaldırılması, gizlenmesi veya kullanıcıların engellenmesi ilgili yetkililer tarafından gerçekleştirilebilir

5.4. Daire Başkanlıkları ve Genel Sekreterlik Sosyal Medya Hesapları

1. Daire Başkanlıkları ve Genel Sekreterlik bünyesinde kullanılan resmi sosyal medya hesapları için birim yöneticisi tarafından yetkili kullanıcı belirlenir.
2. Yetkili kullanıcıların görev ve sorumlulukları belirlenir.
3. Hesaplara erişim yetkileri yalnızca görev gereği ihtiyaç duyan kişilerle sınırlandırılır.
4. Birim faaliyetleri kapsamında hazırlanan;
    - Raporlar,
    - Yazışmalar,
    - Toplantı belgeleri,
    - Personel listeleri,
    - İç yazışmalar,
    - Kurum içi süreç bilgileri,
    - Bilgi güvenliği bilgileri yetkisiz şekilde sosyal medya ortamında yayımlanmaz.

5. Birimlere ait sosyal medya hesaplarında yapılan paylaşımlar Üniversitenin kurumsal iletişim yaklaşımı ve bu politika ile uyumlu olur.

5.5. Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi Sosyal Medya Kullanımı

1. Hastane Bilgi İşlem Biriminde görev yapan personel, görevleri kapsamında eriştiği hasta, çalışan, sistem ve güvenlik bilgilerini kişisel veya resmi sosyal medya hesaplarında paylaşamaz.
2. Hastane bilgi sistemlerine ilişkin;
    - Sunucu bilgileri,
    - Ağ topolojileri,
    - IP adresleri,
    - Güvenlik cihazları,
    - Sistem ekran görüntüleri,
    - Kullanıcı hesapları,
    - Yetkilendirme bilgileri,
    - Zafiyet ve güvenlik açıkları,
    - Log kayıtları,
    - Sistem mimarisi,
    - Teknik yapılandırmalar sosyal medya ortamlarında paylaşılmaz.

3. Hasta veya sağlık verisi içeren ekran görüntüleri, raporlar, fotoğraflar veya videolar sosyal medya hesaplarında yayımlanamaz.
4. Teknik destek veya sorun çözümü amacıyla alınan ekran görüntüleri ve kayıtlar paylaşılmadan önce kişisel veri ve bilgi güvenliği açısından kontrol edilir.
5. Hastane Bilgi İşlem Birimi personeli, sosyal mühendislik veya kimlik avı amacı taşıyabilecek sosyal medya taleplerine karşı dikkatli olur ve şüpheli durumları ilgili bilgi güvenliği süreçlerine bildirir.

5.6. Kişisel Sosyal Medya Hesaplarının Kullanımı

1. Personel ve öğrenciler kişisel sosyal medya hesaplarında yaptıkları paylaşımlardan kendileri sorumludur.
2. Ancak kişisel hesaplarda Üniversiteye ait gizli, kritik veya yetkisiz paylaşılması yasaklanmış bilgiler yayımlanamaz.
3. Denetim, tatbikat, saha çalışması, teknik çalışma, toplantı veya güvenlik uygulamaları sırasında elde edilen ve paylaşılması uygun olmayan fotoğraf, video, belge veya ekran görüntüleri kişisel hesaplarda yayımlanamaz.
4. Personel, kişisel sosyal medya hesabını Üniversitenin resmi hesabı veya resmi sözcüsü izlenimi oluşturacak şekilde kullanamaz.
5. Üniversite adına açıklama yapma yetkisi bulunmayan kişiler Üniversitenin resmi görüşünü açıklayamaz.

5.7. Sosyal Mühendislik ve Kimlik Avı

1. Sosyal medya üzerinden gelen şüpheli bağlantılar, dosyalar, mesajlar ve hesap doğrulama taleplerine karşı dikkatli olunmalıdır.
2. Parola, doğrulama kodu, kullanıcı hesabı veya sistem erişim bilgileri sosyal medya üzerinden talep edilse dahi paylaşılmaz.
3. Üniversite, birim veya hastane adına oluşturulmuş sahte hesapların tespit edilmesi halinde durum ilgili birimlere bildirilir.
4. Sosyal medya üzerinden gerçekleşen şüpheli faaliyetler Olay İhlal Prosedürü kapsamında değerlendirilir.

5.8. Kurum Dışı Depolama ve Mesajlaşma Hizmetleri

Üniversiteye ait gizlilik veya kritiklik değeri bulunan bilgiler;

- Kişisel bulut depolama alanlarında,
- Kişisel e-posta hesaplarında,
- Yetkilendirilmemiş dosya transfer hizmetlerinde,
- Yetkilendirilmemiş mesajlaşma uygulamalarında,
- Sosyal medya mesajlaşma sistemlerinde saklanamaz veya aktarılamaz. Kurum tarafından onaylanmış sistem ve hizmetlerin kullanılması esastır.

5.9. Fikri Mülkiyet ve Telif Hakları

Sosyal medya paylaşımlarında;

- Telif hakları,
- Marka hakları,
- Görsel ve işitsel eser hakları,
- Üniversiteye veya üçüncü kişilere ait fikri mülkiyet hakları korunur. Paylaşılacak içeriklerin kullanım ve paylaşım yetkisi bulunmalıdır.

5.10. Kurumsal İtibar ve Etik Kullanım

Resmi sosyal medya hesaplarında;

- Hakaret,
- Tehdit,
- Ayrımcılık,
- Nefret söylemi,
- Kişileri veya kurumları küçük düşürücü ifadeler,
- Gerçeğe aykırı veya yanıltıcı bilgiler,
- Üniversitenin kurumsal itibarına zarar verebilecek içerikler paylaşılmaz.

Resmi hesaplarda gerçekleştirilecek siyasi, ticari veya diğer özel amaçlı içerikler, ilgili mevzuat ve Üniversitenin yetkilendirme süreçlerine uygun olmak zorundadır.

5.11. İçerik Güvenliği

1. Sosyal medya ortamına yüklenen içeriklerin daha sonra tamamen silinemeyebileceği ve üçüncü kişiler tarafından kopyalanabileceği dikkate alınır.
2. Fotoğraf, video veya ekran görüntülerinde;
    - Kişisel veriler,
    - Hasta bilgileri,
    - Kullanıcı adı,
    - Parola,
    - Doğrulama kodu,
    - Sistem adresi,
    - IP adresi,
    - Gizli belge,
    - Güvenlik bilgisi bulunup bulunmadığı kontrol edilir.

3. Paylaşılması planlanan içerik konusunda tereddüt bulunması halinde paylaşım yapılmadan önce ilgili birim yöneticisine veya yetkili birime danışılır.

6. BİLGİ GÜVENLİĞİ VE KİŞİSEL VERİ İHLALLERİ

1. Sosyal medya kullanımından kaynaklanan bilgi güvenliği ve kişisel veri ihlal olayları Olay İhlal Prosedürü kapsamında değerlendirilir.
2. Hasta verileri veya sağlık verileri içeren bir paylaşımın yetkisiz şekilde gerçekleştirildiğinin tespit edilmesi halinde olay öncelikli olarak ilgili yetkililere bildirilir.
3. İhlalin niteliğine göre erişimlerin kaldırılması, içeriğin kaldırılması, hesap güvenliğinin sağlanması ve gerekli diğer teknik/idari tedbirler uygulanır.
4. Tespit edilen uygunsuzluklar için gerektiğinde Düzeltici ve İyileştirici Faaliyet Prosedürü **uygulanır**.

7. DENETİM VE İZLEME

1. Üniversitenin merkezi resmi sosyal medya hesaplarının yönetim ve kontrolü Kurumsal İletişim Uygulama ve Araştırma Merkezi Müdürlüğü koordinasyonunda yürütülür.
2. Daire Başkanlıkları ve Genel Sekreterlik bünyesindeki resmi hesapların yönetim ve kontrolü ilgili birim yöneticisinin sorumluluğundadır.
3. Araştırma ve Uygulama Hastanesi Bilgi İşlem Birimi tarafından kullanılan resmi hesaplarda bilgi güvenliği ve kişisel veri riskleri ayrıca dikkate alınır.
4. Resmi sosyal medya hesaplarının yetkilendirmeleri belirli aralıklarla ve görev değişikliklerinde gözden geçirilir.

5. Politikanın uygulanmasına ilişkin kontroller; EYS iç tetkikleri, BGYS/KVYS denetimleri, birim kontrolleri ve diğer uygun denetim faaliyetleri kapsamında gerçekleştirilebilir.

8. İHLAL VE YAPTIRIM

1. Bu politika hükümlerinin ihlal edildiğinin tespit edilmesi halinde olayın niteliğine göre ilgili EYS süreçleri işletilir.
2. Uygunsuz içerik veya paylaşımın kaldırılması gerekiyorsa yetkili kişiler tarafından gerekli işlem yapılır.
3. Bilgi güvenliği veya kişisel veri ihlali oluşması halinde ilgili olay yönetimi süreçleri uygulanır.
4. Politika hükümlerine aykırı davranan kişiler hakkında ilgili mevzuat, Üniversitenin disiplin düzenlemeleri ve ilgili EYS prosedürleri uygulanır.