1. AMAÇ

Bu politikanın amacı, bilgi güvenliği risklerini en aza indirmek; hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak; denetim izlenebilirliğini artırmak; bilgi kaynaklarına erişim yetkilerinin güvenli ve kontrollü bir şekilde yönetilmesini sağlayıp yalnızca yetkilendirilmiş kişilerin görevlerine uygun olarak sistemlere erişimini sağlamaktır.

2. KAPSAM

Bu politika, bilgi işleme süreçlerini, bilgi sistemlerini, bilgi varlıklarını ve çalışanları kapsar. Ayrıca, üçüncü taraf hizmet sağlayıcılar ve dış kaynak kullanımı durumları da bu politikanın kapsamına dâhildir.

3. DAYANAK

Bu politikanın temel dayanakları:

- KTÜN TS ISO/IEC ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNERGESİ,
- ISO 27001 standardının aşağıdaki Ek-A Maddeleri:
  - ➢ **A-5.2 Bilgi Güvenliği Rolleri ve Sorumlulukları**: Bilgi güvenliği rolleri ve sorumlulukları organizasyonun ihtiyaçlarına göre tanımlanmalı ve atanmalıdır.
  - ➢ **A-5.3 Görevlerin Ayrılması**: Çakışan görevler ve sorumluluk alanları ayrılmalıdır.
  - ➢ **A-5.15 Erişim Kontrolü**: Bilgi ve diğer ilgili varlıklara fiziksel ve mantıksal erişimi kontrol etmek için kurallar, iş ve bilgi güvenliği gereksinimlerine dayalı olarak oluşturulmalı ve uygulanmalıdır.
- CDDO Bilgi ve İletişim Güvenliği Rehberi
- ilgili diğer mevzuattır.

4. TANIMLAR

KTÜN / Üniversite: Konya Teknik Üniversitesi.

BİDB: Bilgi İşlem Daire Başkanlığı.

Görevler Ayrılığı İlkesi: Hiçbir çalışanın, bir işlemin başlangıcından tamamlanmasına kadar geçen süreçte, birden fazla kritik sorumluluk almamasıdır. Bir çalışan aynı süreç içinde hem yürütme, hem onaylama hem de denetim gibi kritik işlevleri yerine getirmemelidir.

Erişim Kontrol Sistemleri: Bir kullanıcının yapmaya yetkisi olmayan bir işlemi yapmak istese bile bunu engelleyen sistemlerdir. Bir organizasyonun kaynaklarına, sistemlerine veya fiziksel alanlarına kimlerin, nasıl ve ne zaman erişebileceğini belirlemek, yönetmek ve izlemek için kullanılan mekanizma ve teknolojilerdir. Bu sistemler, **dijital bilgiye** (ör. veritabanı, uygulama) ve **fiziksel yerlere** (ör. binalar, sunucu odaları) yetkisiz erişimi önlemek amacıyla tasarlanmıştır

Yetkilendirme: Bir çalışana veya bir ekibe belirli görev veya eylemleri gerçekleştirme izninin verilmesi.

Denetim İzlenebilirliği: Sistem veya süreçte, teoride yapılması gereken ve fiiliyatta yapılan işlemlerin izlenebilir olmasını sağlayan kayıt mekanizması.

Minimum erişim ilkesi: Bir kullanıcının, sistemin, uygulamanın veya sürecin işini yerine getirebilmesi için ihtiyaç duyduğu **en az yetkiye** sahip olması gerektiğini savunan bir güvenlik ilkesidir. Bu ilke, yetkisiz erişim risklerini ve potansiyel zararları en aza indirmek amacıyla uygulanır. Gereksiz veya aşırı erişim izinleri, güvenlik açıklarına yol açabilir. Bu ilke, yetkisiz erişimi engeller, iç tehdit riskini azaltır, saldırganların hareket alanını kısıtlar.

Çift Kontrol ile Doğrulama: Çift kontrol ile doğrulama (Dual Control), kritik işlemlerin tamamlanabilmesi için birden fazla kişinin onayına veya katılımına ihtiyaç duyulmasını ifade eden bir güvenlik mekanizmasıdır. Bu yaklaşım, özellikle hassas işlemlerin, kaynakların veya verilere erişimin kontrol edilmesi ve güvence altına alınması için kullanılır. Örneğin:

- Organizasyonlarda kritik politika veya prosedür değişiklikleri için ilgili birim yöneticilerinin ortak karar alması.
- Hassas verilerin geri yüklenmesi veya tamamen silinmesi için birden fazla kişinin onayına ihtiyaç duyulması.
- Kritik veri merkezlerinde hem sistem yöneticisinin hem de güvenlik görevlisinin onayının gerekmesi.

5. SORUMLULAR

Bu politikanın hazırlanmasından BİDB, onaylanmasından BGYS komisyonu, uygulanmasından tüm amirler ve personel ile KTÜN sistemlerine erişim sağlayan üçüncü taraflar sorumludur.

Amirlerin sorumlulukları:

- Süreçlerin, görevler ayrılığı ilkesine uygun olarak tasarlanmasını ve yürütülmesini sağlar.
- Politikanın ihlal edilmesi durumunda gerekli aksiyonları alır ve raporlama yapar.
- Erişim kontrolü ve izleme mekanizmalarının kurulup uygulanmasını sağlar.
- Erişim ihlallerini araştırır ve gerekli önlemleri alır. Politikalarının etkinliğini değerlendirir.
- Görevler ayrılığı ve erişim kontrolü ile ilgili denetimlere destek sağlar.

Tüm personelin ve üçüncü tarafların sorumlulukları:

- Politikanın hükümlerine uygun davranmak ve görevlerini belirlenen sınırlar içerisinde görevler ayrılığı ilkesine riayet ederek yerine getirmekle sorumludur.
- Kendilerine atanmış olan görevlerde yalnızca yetkili oldukları alanlarda çalışmalı ve diğer operasyonel süreçlere müdahale etmemelidir.
- Parola ve diğer kimlik doğrulama bilgilerini güvenli tutmalıdır.
- İlgili eğitimlere katılmalı ve politikaların uygulanmasında aktif bir rol almalıdır.
- Yetkisiz erişim veya görevler ayrılığına aykırı durumları tespit ettiklerinde ilgili amire bilgi vermekle yükümlüdür.

6. HEDEFLER

6.1. Görevlerin Ayrılması

Görevlerin ayrılmasıyla, bir organizasyonda riskler minimize edilerek, hataların ve suistimallerin önlenmesi amacıyla kritik işlemlerin birden fazla kişi veya ekip arasında paylaşılması sağlanır. Görevler ayrılığı, organizasyonel güvenliği, verimliliği ve uyumu güçlendiren kritik bir ilkedir.

6.2. Suistimalleri ve Hileyi Engelleme

Görevlerin ayrılması, bir kişinin tek başına tüm süreci kontrol etmesini engeller. Bu, kişisel veri ihlallerinin, finansal suistimallerin, hileli işlemlerin ve kötü niyetli hareketlerin önüne geçer. Örneğin, bir kişi aynı anda ödeme talebini oluşturup, ödeme işlemini onaylayamaz.

6.2.1. Hataların Tespiti ve Düzeltilmesi

Aynı işlemi birden fazla kişi kontrol ederse, hataların tespiti daha kolay olur. Bir kişi işlemi yaparken diğeri gözden geçirebilir, böylece yanlışlıkların erken aşamada fark edilmesi sağlanır.
"**Çift Kontrol ile Doğrulama"** sayesinde özellikle önemli işlemler, bir kişinin yalnızca başlatması ve diğerinin onaylaması ile doğrulanır.

6.2.2. İç Kontrolün Güçlendirilmesi

Organizasyondaki iç kontrol ve denetim süreçlerini güçlendirir. Her bir işlevin farklı kişiler arasında dağıtılması, kontrolün daha etkili bir şekilde yapılmasını sağlar. Etkin izleme ve gözetim, hangi işlemi kimin yaptığını izlemeyi kolaylaştırır ve olası hataları ya da usulsüzlükleri hızlıca tespit eder.

6.2.3. Yasal Uyumun Sağlanması

Birçok mevzuat, görevler ayrılığı ilkesine uyulmasını zorunlu kılar. Görevlerin ayrılması, hem iç hem de dış denetimlerde, denetçilerin işlemler hakkında güvenli ve net bir şekilde raporlama yapabilmesini sağlar. Bu da yasal uyumun sağlanmasında büyük rol oynar.

6.2.4. İş Süreçlerinde Etkinlik ve Verimlilik

Görevler ayrılığı, organizasyonel süreçlerin daha düzenli ve verimli bir şekilde işlemesini sağlar. İki kişinin birbirini denetlemesi, daha doğru ve hızlı kararlar alınmasını sağlar.
Personel, sadece kendi sorumluluklarını yerine getirecek şekilde organize olur, bu da kaynakların daha etkin kullanılmasını sağlar. Örneğin, bir kişi sadece ödeme işlemleriyle ilgilenirken, bir diğer kişi sadece raporlama yapabilir.

6.2.5. İzlenebilirlik ve Denetim İzleri(Kayıtları)

Görevler ayrılığı, organizasyonların her işlevi için denetim izlerinin tutulmasını sağlar. Bir işlemi başlatan, onaylayan ve tamamlayan kişilerin kim olduğunun açıkça belirlenmesi işlemlerin izlenebilirliğini artırır ve her aşamanın takip edilmesini ve şeffaflığı sağlar.

6.2.6. Erişim Kontrollerinin İyileştirilmesi

Her kullanıcının yalnızca kendine ait olan görevleri yerine getirmesi sağlanır. Bu, bilgi sistemlerine yapılan erişimlerin kontrol edilmesine yardımcı olur. Kullanıcılar sadece işlerini yapacak kadar bilgiye erişerek(minimum yetki ilkesi) yetkisiz erişimler önlenir, gizlilik sağlanır bu da organizasyonun hassas bilgilerini korur. Erişim yetkilerinin düzenli olarak gözden geçirilmesi sağlanır. Erişim loglarının düzenli olarak izlenmesini ve kayıt altına alınması sağlanır.

6.2.7. Performans Değerlendirmeleri ve Görev Dengelemesi

Görevlerin ayrılması, çalışanlar arasında adil bir görev dağılımı sağlar. Bu, her çalışanın yalnızca kendi sorumluluk alanındaki işlemleri yapmasına olanak tanır, dolayısıyla performans değerlendirmeleri daha objektif olur.

İş yükü eşit şekilde dağıtıldığı için, çalışanlar arasında dengesiz bir yük oluşturmaz ve bu da motivasyonu artırır.

6.2.8. Kriz Durumlarında Hızlı Müdahale

Görevler ayrılığı sayesinde, bir çalışan işten ayrıldığında veya geçici olarak devamsız olduğunda, diğer çalışanlar hızla yerini alabilir.

Herkesin belirli görevleri olması, krizde bile işlerin aksamadan devam etmesini ve iş sürekliliğini sağlar. Kriz sırasında oluşabilecek farklı senaryoları önceden analiz ederek hızlı aksiyon planları oluşturmak kolaylaşır. Krizde hızlı müdahaleyi sağlamak için yalnızca ilgili çalışanlara belirli bir süreliğine ek erişim izinlerinin verilmesi, bu erişimlerin denetim altına alınmasını kolaylaştırır.

Görevler ayrılığı ilkesine uygun olarak, birbirini yedekleyebilecek şekilde eğitim almış personelin kriz ekiplerinde görevlendirilmesi sağlanır.

7. UYGULAMA

7.1. Görevlerin Tanımlanması

7.1.1. Kritik bilgi güvenliği süreçlerinde, görevler ayrılığı ilkesi uygulanmalı ve bir görev tümüyle tek bir kişi tarafından yürütülmemelidir. Personel sayısının yetersizliği nedeniyle görevler ayrılığı ilkesinin tam olarak uygulanamadığı idarelerin yöneticileri risklerin farkında olmalı ve gerekli önlemleri almalıdır.

7.1.2. Organizasyonel süreçler ve iş akışları analiz edilerek ayrılması gereken görevler tespit edilmeli ve her süreçte hangi işlemin hangi ekip tarafından yapılacağı net bir şekilde belirlenmelidir. Özellikle yüksek risk taşıyan işlemler için hangi işlemler arasındaki birleşimin risk oluşturduğu belirlenerek, bu işlemler için ayrı görevler tanımlanmalıdır. Örneğin yazılım geliştirenler ile geliştirilen yazılımın testini yapanlar ayrılmalı ya da bir sistemin "yedek alma" işlemi için "yedekleme" ve "yedekten geri alma testi" olmak üzere iki farklı görev tanımlanmalıdır.

7.1.3. Her iş pozisyonu için bilgi güvenliğiyle ilişkili sorumluluklar iş tanımına dahil edilmelidir.

7.2. Rol ve Sorumlulukların Tanımlanması

7.2.1. RACİ Matrisi:

7.2.1.1. Bilgi güvenliğiyle ilgili sorumluluk ve yetkiler net bir şekilde tanımlanmalı ve atanan roller çatışmalara neden olmayacak şekilde düzenlenmelidir. Görevlerin ayrımıyla ilgili ilkeler, bilgi güvenliği politikasının parçası olarak uygulanmalıdır.

7.2.1.2. Ekipler ve ekiplerin görevlerinin yer aldığı RACI matrisi oluşturulmalıdır.

7.2.1.3. Matriste her satır ayrı bir görevi her sütun da ayrı bir ekibi temsil etmelidir.

7.2.1.4. Görevlerin ve ekiplerin kesiştiği her hücre için aşağıdaki harflerden birisi girilmelidir, hiçbirine uymayanlar boş bırakılmalıdır:

- **R:** Sorumlu (-R- Responsible / İşi-görevi Yapmakla Sorumlu)
- **A**: Onaylayan (-A- Accountable Yönetici / Genel Sorumlu / Kontrol Eden)
- **C**: Danışılan (-C- Consulted Karar verme sürecinde bilgi ve görüş sağlayan, sürecin başarısını etkileyebilecek uzmanlığa sahip aktif bir rol)
- **I**: Bilgilendirilen (-I- Informed Karar verildikten veya görev tamamlandıktan sonra sonuçlardan haberdar edilen pasif bir roldür. Karar sürecine aktif olarak katılmaz, yalnızca sonuçlardan haberdar edilir.)

7.2.1.5. RACİ matrisinde bir satırda sadece bir tane **sorumlu**(R) ve en az bir tane **onaylayan**(A) olmalıdır. Tüm görevlerin sorumluları netleştirilmelidir. Görevler, bir iş için birden fazla sorumlu ekip olmayacak şekilde atomize edilmelidir.

7.2.1.6. Matris, kritik görevlerin farklı kişiler tarafından yürütüldüğünü açıkça göstermelidir. Örneğin RACİ matrisindeki bir hücrede hem Sorumlu(R) hem de Onaylayan(A) aynı anda bulunmamalıdır. Bir işi "**yapan** ile **kontrol edip onaylayan**" farklı kişiler olmalıdır.

7.2.1.7. Her çalışan için hangi ekiplerde olacağı net olarak belirlenmelidir. Birleşimi risk oluşturduğu için ayrı görevler olarak tanımlanan işlemlere ait ekiplerde aynı kişilerin olmadığından emin olunmalıdır. Her çalışana, hangi ekiplerde yer aldığı, görev tanımları ve RACİ matrisinin olduğu dökümanlar tebliğ edilmelidir.

7.2.1.8. RACİ matrisi kontrolleri **en fazla 6 ayda bir** olmak üzere düzenli olarak gözden geçirilmelidir. Bir çalışanın görevlerinde bir değişiklik olduğunda en kısa sürede matris güncellenmeli ve ilgililerine tebliğ edilmelidir.

7.2.1.9. Görevlendirme veya görev iptal süreçlerinin kaydı tutulmalıdır.

7.2.1.10. Tüm çalışanlara ve ilgili paydaşlara, kendi rollerine uygun güvenlik politikaları ve sorumlulukları konusunda eğitim verilmelidir.

7.2.2. Ekipler Arası Çakışma Matrisi:

7.2.2.1. Görevler ayrılığı ilkesini uygulayabilmek için "Ekipler" ve "Ekiplerin Görevleri" belirlendikten sonra bir kişinin aynı anda hangi ekiplerde bulunup hangilerinde bulunamayacağının net olarak belirtilmesi gerekmektedir.

7.2.2.2. Bir tablonun hem satır hem de sütunlarına aynı sırada tüm ekip isimleri yazılır ve her hücre için bu hücreye karşılık gelen satır ve sütundaki ekipler için bir kişi aynı anda bu ekiplerin her ikisinde de yer alabiliyorsa "Uygun" alamıyorsa "Uygun Değil" veya risk durumuna göre "Kesinlikle Uygun Değil" şeklinde işaretlenmelidir.

7.2.3. Erişim Yetkileri Matrisi:

7.2.3.1. Bilgi ve diğer ilgili varlıklara fiziksel ve mantıksal erişimi kontrol etmek için kurallar, iş ve bilgi güvenliği gereksinimlerine dayalı olarak oluşturulmalı ve uygulanmalıdır. Kullanıcılar sadece görevlerini yerine getirmek için ve sadece ihtiyaç duydukları sistemlere, verilere veya uygulamalara erişim sağlayabilmelidir.

7.2.3.2. Görevler ayrılığı ilkesinin etkili bir şekilde uygulanabilmesi için, **Erişim Kontrol Sistemleri**, doğru şekilde yapılandırılmalıdır. Kullanıcıların yalnızca kendi görevleriyle ilgili işlem yapmalarına olanak tanıyacak şekilde yetki sınırları belirlenmelidir. Örneğin sistem odası biyometrik kapı geçiş sisteminde sadece bu konuda görevlendirilmiş personel tanımlı olmalıdır.

7.2.3.3. Kullanıcıların yalnızca işlerini yapmak için gereken asgari erişime sahip olduklarından emin olunmalıdır(**Minimum Erişim İlkesi**).

7.2.3.4. Sistemlere erişim, güçlü kimlik doğrulama mekanizmalarıyla korunmalı, parola politikası uygulanmalı, iki faktörlü kimlik doğrulama (2FA) gibi ek güvenlik önlemleri kritik sistemler için zorunlu tutulmalı, parolalar asla paylaşılmamalı ve belirli periyotlarda parola değişimi zorunlu tutulmalıdır.

7.2.3.5. Tedarikçi ve dış kullanıcı erişimleri yalnızca gerekli durumlarda ve iş tanımı çerçevesinde sağlanır.

7.2.3.6. Tedarikçilerin erişimi, sözleşmede belirtilen güvenlik önlemleri çerçevesinde sınırlandırılır ve denetlenir.

7.2.3.7. Sistemlerdeki erişim kontrolleri **en fazla 3 ayda bir** olmak üzere düzenli olarak gözden geçirilerek artık gerekli olmayan veya uygunsuz erişim yetkileri iptal edilmelidir. Bir çalışan pozisyon değiştirirse veya işten ayrılırsa, o kişinin eski yetkileri en kısa sürede iptal edilmelidir.

7.2.3.8. Tüm erişim faaliyetleri, uygun loglama sistemleriyle kayıt altına alınmalı, loglar, düzenli olarak izlenmeli ve anormal aktiviteler derhal rapor edilmelidir.

7.2.3.9. Tüm erişim istekleri yazılı olarak belgelenmeli ve hem talebi yapan hem de yerine getiren ilgili birim yöneticilerinin onayı alınmalıdır.

7.2.3.10. Üzerinde erişim yetkisi tanımlanan tüm sistemler (yazılım, donanım veya manuel kontrollü süreçler) için yapılan erişim ayarlamaları hakkında aşağıdaki detay bilgileri

içeren kayıtlar(Erişim Yetkileri Matrisi veya bu işi yapan yazılım ile) tutulmalı ve "**Erişim Yönetimi Prosedürü**"nde bu sistemler belirtilmelidir:

* **Kullanıcı (veya ekip) Adı:** Kendisine yetki verilen kişi veya grup.
* **Varlık/Süreç Adı**: Kullanıcının erişim sağladığı sistemler (yazılım, donanım veya manuel kontrollü süreçler). Manuel kontrollü sürece örnek olarak "bir alana girişin güvenlik personelince kimlik bilgilerine bakılarak kontrol edilip sadece önceden güvenlik personeline verilen listede olanların alana alınması süreci" verilebilir.
* **Erişim Seviyesi:** Hangi tür erişime sahip olduğu (Örnek: Görüntüleme, Düzenleme, Silme, Yükleme).
* **Onaylayan Personel:** Bu erişimi onaylayan kişi veya departman (ör. Bilgi İşlem Daire Başkanı).
* **Yetkilendiren Personel:** Bu erişim iznini veren veya izin için gerekli ayarları ilgili yazılım veya donanıma giren. (ör. Sistem Yöneticisi).
* **Talep Bilgisi:** Yetkilendirme talebinin hangi birimden ve kimden hangi yazılı belge ile geldiği belirtilmelidir.
* **Erişim Nedeni:** Kullanıcının bu erişime neden ihtiyaç duyduğu (ör. İş rolü gereksinimi, proje kapsamı).
* **Başlangıç Tarihi:** Erişim yetkisinin başlangıç tarihi.
* **Bitiş Tarihi:** Geçici erişim durumunda bitiş tarihi (ör. Proje bazlı erişim).
* **Denetim Durumu:** Erişim yetkisinin en son ne zaman gözden geçirildiği (ör. Denetim tarihi ve sonucu).

7.2.4. Görev Dağılımı ve Vekalet Matrisi:

7.2.4.1. Vekalet tablosu, bir çalışanın bulunamadığı durumlarda, görev ve sorumluluklarının devredileceği kişileri tanımlayan bir dokümandır. Bu tablo, özellikle kritik bilgi güvenliği süreçlerinin aksamaması ve kurumsal sürekliliğin sağlanması amacıyla kullanılır. Görevlerin ayrılığı ilkesine uygun şekilde vekalet planlaması yapmak önemlidir. Hazırlanmaması durumunda, bilgi güvenliği süreçleri ve iş sürekliliği riske girebilir. Kritik görevlerde bir yetki boşluğu oluşabilir, bu da güvenlik açıklarına ve aksamalara yol açabilir.

7.2.4.2. Vekalet Matrisinin Önemi:

Süreklilik Sağlanması: Bilgi güvenliği süreçlerinin kesintiye uğramaması için görev devrini mümkün kılar.

Risk Yönetimi: Acil durumlarda görevlerin kimin tarafından üstlenileceğini netleştirerek belirsizliği önler.

Sorumluluk Takibi: Görev devrinin kayıt altına alınması, sorumlulukların izlenebilirliğini artırır.

Uyumluluk: ISO 27001'in iş sürekliliği ve sorumluluk yönetimi prensipleriyle uyumlu bir yapıyı destekler.

7.2.5. Vekalet matrisi hazırlanırken tanımlanan tüm görevler için en az bir yedek kişi atanmalı, tercihen iki yedek belirlenmelidir. Matriste aşağıdaki detay bilgileri içeren kayıtlar tutulmalı ve görev tanımları ile birlikte ilgili personele tebliğ edilmelidir:

Görev/Ekip Adı	Ana Sorumlu	Ana Sorumlu Vekili (1. Yedek)	Diğer Ekip Üyeleri

8. GÖZDEN GEÇİRME VE REVİZYON

Bu politika, yılda en az bir kez gözden geçirilir ve gerektiğinde güncellenir. Ayrıca, organizasyondaki önemli değişiklikler veya ISO 27001 standardındaki güncellemeler dikkate alınarak revizyon yapılır.

9. YAPTIRIM

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen "POLİTİKANIN İHLALİ VE YAPTIRIMLAR" başlığı altındakiler geçerlidir.

10. YÜRÜRLÜK

Bu politika, Konya Teknik Üniversitesi Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

11. YÜRÜTME

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.