BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ ve HEDEF

Bu Politikanın amacı; Kurumun faaliyetlerinde kullandığı bilgi sistemlerinin yönetiminde esas alınacak ilkeler ile bilgi sistemlerinin kullanımından kaynaklanan risklerin tanımlanması, ölçülmesi, izlenmesi, kontrol edilmesi, raporlanması ve etkin bir şekilde yönetilmesine ilişkin esasları belirlemektir.

Politikanın hedefi; her seviyede kullanıcıya bilgi sistemleri kullanımları sırasında ne şekilde hareket etmeleri gerektiği konusunda yol göstermek, kullanıcıların bilinç ve farkındalık seviyelerini artırmaktır. Böylece bilgi sistemlerinde oluşabilecek riskleri minimuma indirmek, Kurumun güvenilirliğini ve imajını korumak, Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamaktır.

2. KAPSAM

Bilgi sistemleri varlıklarını, bunların sorumluklarını ve süreçleri kapsar.

3. TANIMLAR

Bilgi Sistemleri: Elektronik ortamda bilgilerin işlenmesi ve depolanması için kullanılan giriş, işleme, depolama, yedekleme, kopyalama ve yazdırma fonksiyonlarını kapsayan yazılım ve donanımlar.
Bilgi Güvenliği: Bilgi sistemleri üzerinde işlenen, depolanan bilgilerin erişilebilirliğinin, bütünlüğünün ve gizliliğinin sağlanması.
BSGS: Bilgi Sistemleri Güvenliği Sorumlusu. Bilgi sistemlerinin yönetimine ve bilgi güvenliğinin sağlanmasına ilişkin Üst Yönetimce hazırlanmış ve Yönetim Kurulu tarafından onaylanmış Bilgi Güvenliği Politikasının, Risk Yönetim Prosedürleri ve Süreçlerin tesis edilmesi, bilgi teknolojilerinin kullanılmasından kaynaklanan risklerin etkin biçimde yönetilmesini sağlayan Kurum sorumlusu.
KVK: Kişisel Verilerin Korunması.

4. BİLGİ SİSTEMLERİ GÜVENLİĞİNE İLİŞKİN TEMEL İLKELER

Bilgi sistemlerinin yapısının, Kurumun ölçeği, faaliyetlerin niteliği ve stratejik hedefleri ile uyumlu olması; bilgi sistemleri ile içerdiği verinin güvenilir, doğru, eksiksiz, bütünlüğü sağlanan, izlenebilir, tutarlı, erişilebilir ve ihtiyaçları karşılayacak nitelikte oluşturulması esastır.

Bilgi sistemleri asgari olarak;

- Kurumla ilgili tüm bilgilerin elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanılmasına, yedeklenmesine ve kullanılmasına,
- Risk ölçüm yöntemleri kullanılarak risklerin ölçülebilmesine ve zamanında ve etkin bir şekilde raporlanabilmesine,
- Bilgi sistemlerine ilişkin yılda en az bir defa risk analizi yapılması ve bilgi sistemlerinde meydana gelebilecek önemli değişikliklerde tekrarlanmasına,
- Bilgi sistemleri güvenliğinde rollerin ve sorumlulukların açıkça belirlenerek çalışanlara bildirilmesine,
- Kişisel Verilerin Korunması Kanunu ve Yönetmelikleri ile Kurumumuzun KVK ile ilgili Politika ve Prosedürlerin Kurum içinde etkin ve düzenli bir şekilde uygulatılmasına,

- Sunulan hizmet ve faaliyetlere ilişkin kaynak tahsisinin Kurumun risk alma düzeyine göre belirlenmesine,
- Muhasebe kayıtlarının Kanun ve Yönetmeliklerle belirlenen usul ve esaslara uygun şekilde muhasebeleştirilmesine

imkân verecek yapıda tesis edilir.

5. SÜREÇLERDEKİ ROLLER VE SORUMLULUKLAR

Üst Yönetim Sorumlulukları

- Bilgi sistemleri güvenliğine ilişkin Süreç ve Prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda Üst Yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir Bilgi Sistemleri Güvenliği Sorumlusunu belirlemek,
- Bilgi güvenliği faaliyetleri ile ilgili gerekli kaynağı tahsis etmek,
- Bilgi Güvenliği Politikasını, görev ve sorumlulukları belirlemek, her yıl Politikayı güncellemek, Yönetim Kurulu onayına sunmak ve Kurum içinde uygulanmasına destek vermek,
- Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin hazırlanan projeleri gözden geçirmek ve ihtiyaca göre uygun olanları onaylamak,
- Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetimini gerçekleştirmek,
- BSGS tarafından hazırlanan Risk Analiz Raporlarında kritik seviyedeki risklere karşı önlemleri onaylamak, bilgi güvenliği ihlallerine ilişkin olayları izlemek ve her yıl değerlendirmek,
- Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaları yapmak ve eğitimlerin verilmesini sağlamak,
- Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için İş Sürekliliği Planı hazırlamak,
- Bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi Yönetim Kurulu'nun sorumluluğundadır.

Birim Müdürlerinin Sorumlulukları

- Kendisine bağlı çalışan personelin tüm bilgi işlem uygulama yetkilerini ve değişikliklerini e-posta yoluyla BSGS'na bildirerek onaylamak,
- Fark ettiği veya kendisine çalışanları aracılığıyla iletilen bilgi sistemleri ile ilgili güvenlik problemlerini BSGS'na bildirmek,
- Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncelleme talebinde bulunmak,
- Kendi yöneticisi olduğu Birimde Bilgi Güvenliği Politikasının etkin ve düzenli bir şekilde uygulanmasını sağlamak.

BSGS Sorumlulukları

- Farkındalık eğitimlerini planlamak ve gerçekleşmelerini sağlamak,
- Güvenlik risklerini minimize etmek, verilerin gizliliğini, bütünlüğünü ve erişebilirliğini sağlamak, faaliyetlerin düzgün bir şekilde devamı için iş sürekliliğini sağlamak, bilgi sistemlerinin performansını ölçmek için her yıl çeşitli kontroller ve testler yapmak,
- Yeni bilgi sistemleri edinimleri, iyileştirmeler ve geliştirmeler öncesinde testleri yapmak, proje geliştirme raporları oluşturmak ve bunu Üst Yönetim onayına sunmak,

- Bilgi güvenliği ile ilgili konularda çalışanlar ve dış hizmet sağlayıcılar arasında koordinasyonu sağlamak, bilgi sistemlerini dış hizmet veren tarafları Bilgi Güvenliği Politika ve Prosedürlerinden haberdar etmek, Dış hizmetler için hizmetin erişilebilirliğini, performansını ve sözleşmeye uygunluğunu takip etmek,
- Bilgi Sistemleri İş Sürekliliği Planı'nın uygulanmasını ve güncellenmesini sağlamak,
- Birim Müdürlerinin kendisine bağlı personelin tüm bilgi işlem uygulama yetkileri ve değişikliklerini onayladığı e-postayı aldıktan sonra gerekli yetkileri tanımlamak,
- Güvenlik zaafları ve ihlallerin nedenlerini araştırmak, delilleri saklamak, Üst Yönetime önlemler ve iyileştirme önerilerinde bulunmak ve durumları raporlamak,
- Bilgi sistemlerinin fiziksel güvenliğini sağlamak,
- Bilgi güvenliği ile ilgili denetim iz kayıtlarını tutmak, saklamak, yetkilendirmeleri yapmak, kaydetmek ve takip etmek, çalışanları sürekli bilgilendirmek ve uyarmak,
- Kurumun teknolojik gelişmelere uyumunu sağlamak, bilgi sistemleri sürekliliğini ve güncelliğini sağlamak,
- Sızma Testi ve Bilgi Güvenliği Bağımsız Denetiminde denetleyici Kurum veya yetkililere gereken tüm desteği vermek,
- Bilgi sistemleri envanterini risk derecesine göre sınıflandırarak oluşturmak ve güncelliğini sağlamak,
- Bilgi sistemleri güvenliğiyle ilgili riskleri belirlemek ve bu risklerin yönetilmesini sağlamak, risk analizlerini yapmak ve Üst Yönetime rapor sunmak.

Üst Yönetimin aksi bir kararı olmadıkça Kurumun Bilgi İşlem Birimi Sorumlusu Bilgi Sistemleri Güvenliği Sorumlusudur.

Kurum Çalışanlarının Sorumlulukları

- Çalışanlar için hazırlanmış roller ve sorumluluklarla ilgili dokümanlarda belirtilen görevleri yerine getirmek, kurallara uymak,
- Görevlerini gerçekleştirmek için kendilerine verilmiş olan ayrıcalıklı yetkileri var ise bu yetkileri ve hakları sadece bu işi yaparken kullanmak,
- Erişim ve kullanım yetkisi bulunan bilgi varlığını korumak, herhangi bir hata/arıza/olay olduğunda Birim Yöneticisine ve BSGS'na bilgi vermek,
- Bilgi Güvenliği Politika ve Prosedürlerine uymak,
- Farkındalık eğitimlerine katılmak, alınan eğitimlere riayet etmek,
- Herhangi bir bilgi güvenliği ihlalini fark ettiğinde, zaman geçirmeden Birim Yöneticisine ve BSGS'na bilgi vermek,
- Kendisine ait olan hesapların şifrelerinin (varsa e-anahtarının) güvenliğini sağlamak,
- Taşınabilir cihazların güvenliğini sağlamak, yetkilendirme olmadan dışarı bilgi varlığı çıkarmamak,
- Kişisel Verilerin Korunması Kanunu ve Yönetmelikleri ile Kurumun KVK ile ilgili tüm Politika ve Prosedürlerine uymak ve bu doğrultuda Kuruma ait bilgi varlıklarının ve kişisel verilerin korunmasını sağlamak.

3. Taraf Sorumlulukları

- 3. taraf olduğu Kurumun Bilgi Güvenliği Politikası ve Prosedürlerine uymak,
- Taahhüt ettiği Sözleşme hükümlerine ve Kuruma ait bilgi varlıklarının ve kişisel verilerin korunmasına riayet etmek, görevi gereği Sızma Testi veya Bilgi Sistemleri Bağımsız Denetimi veya bilgi sistemleri bakım, onarım veya tesisinde tüm gerekenleri tarafsız, güvenilir, eksiksiz ve etkin bir şekilde yerine getirmek,

- Bilgi sistemlerinin sağlıklı işlemesi için gerekli görülen önerileri ve ihlal olaylarını ilgili kişiye iletmek.

6. BİLGİ SİSTEMLERİ GÜVENLİĞİ ÇALIŞMA ESASLARI

- Bilgi sistemleri ile içerdiği verilerin gizliliğini, güvenliğini, bütünlüğünü, erişebilirliğini ve doğruluğunu sağlamak için yönetim sistemi ve süreçler oluşturulur. Söz konusu sistem ve süreçlerin işlerliği ve yeterliliği test edilir, test sonuçları izlenir, raporlanır ve gerekli tedbirler alınır.

  Bilgi Güvenliği Yönetim Sistemi bilgi ve bilgi varlıklarının gizliliği, bütünlüğü ve erişebilirliği ilkeleri üzerine inşa edilmiş ve risk yaklaşımına dayanan bir yönetim sistemidir.

  Gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması veya bilginin yetkisiz kişilerce açığa çıkarılması ve paylaşılmasının engellenmesidir.
  Bütünlük, bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük, yanlışlıkla veya kasıtlı olarak bilginin bozulmamasıdır.
  Erişebilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişebilirliği kullanıcıların yetkileri çerçevesinde olmalıdır. Erişebilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.
- Bilgi sistemlerinin sürekli biçimde işlerliğini sağlamak üzere İş Sürekliliği Planı oluşturulur. Söz konusu Planın işlerliği ve yeterliliği düzenli olarak test edilir; ihtiyaç duyulması halinde gerekli tedbirler alınır. Bilgi Sistemleri İş Sürekliliğinin Planlanması, bilgi varlıkları risk sınıflandırması yapılarak belirlenir; bunlara ilişkin iş etki analizi ile risk değerlendirmesi yapılır ve gerektiğinde güncellenir.
  Bilgi Varlığı; Bir Kurum için değeri olan ve bu nedenle uygun olarak korunması gereken unsurlardır.

  - Kurum bünyesinde kullanılmakta olan her bir bilgi varlığı, envanter kayıtlarına geçirilmelidir.
  - Envanter kayıtları sürekli olarak güncel tutulmalı ve yeni bilgi varlıkları, envanter kayıtlarına hemen girilmelidir.
  - Bilgi Varlıkları kapsamında değerlendirilen bilgi, yazılım, donanım ve hizmet varlıkları için sorumlular atanmalı ve varlıkların sorumluları, envanter kayıtlarında bulunmalıdır.
  - Herhangi bir bilgi teknolojisi varlığının sahibi olarak belirlenmiş personel, bu varlığın korunmasından sorumludur.
  - Bilgi varlıklarının sınıflandırılmasından ve bu sınıflandırmanın belirli zamanlarda gözden geçirilmesinden BSGS sorumludur.
  - Erişim kontrol ve ağ hizmetleri kullanımı ve risk yönetimi hazırlanırken varlık envanteri listesi göz önünde bulundurulmalıdır.

- Bilgi sistemleri ile içerdiği verinin güvenli biçimde saklanması esastır. Bu çerçevede, veriler, güvenlik hassasiyet derecelerine göre sınıflandırılır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir ve buna göre yedeklenir. Bilgi sistemlerinin güvenliği ve yedekleme sistemlerinin işleyişi düzenli olarak test edilir ve test sonuçlarına göre ihtiyaç duyulması halinde gerekli değişiklikler gerekli üst yönetim onayları alındıktan sonra yapılır.
- Performans değerlendirildikten sonra kapasite artırımı ihtiyacı varsa BSGS tarafından üst yönetim bilgilendirilir; ön onay alındıktan sonra alınan teklifler üst yönetim onayına sunulur. Onaylanması durumunda kapasite ve performans artırımı için gerekli satın alma ve iyileştirmeler gerçekleştirilir.
- Bilgi güvenliğinin temininde ve Kurumun bilgi sistemlerine erişimde, kimlik doğrulama ve yetkilendirme mekanizmaları ve sorumluluk atama imkânlarını içeren teknikler kullanılır.

- Kurumumuzda anahtar yönetimi çerçevesinde SSL algoritmik şifreleme uygulaması kullanılmaktadır. Bu sertifika uluslararası standartlara sahiptir. SSL sertifikaları güvenliği için uluslararası otoriteler tarafından sertifika süreleri 1 yıl olarak kısıtlandırıldığından her yıl güncellenmektedir. Şifreleme tekniğinin geçerliliğini yitirmesi söz konusu olursa bundan önce her yıl sertifika bitiş süresi dolmadan yeni bir sertifika satın alınarak sisteme entegre edilecektir.
- Bilgi sistemlerinin geliştirilmesi, test edilmesi ve işletilmesi süreçlerinde görevler ayrılığı ilkesi uygulanır. Bilgi sistemleri yönetim sürecinde tüm çalışanların görev, yetki ve sorumlulukları belirlenir. Görev ve sorumluluklar belirli aralıklarla gözden geçirilir ve güncelliği sağlanır. Bilgi sistemleri süreçleri tasarlanırken kritik işlemlerin tek bir personele veya dış kaynak hizmeti sunan kuruluşa bağımlı olmaması göz önünde bulundurulur. Görevlerin tam ve uygun şekilde ayrılmasının mümkün olmadığı durumlarda oluşabilecek hata, eksiklik veya kötüye kullanımı önlemeye ve tespit etmeye yönelik telafi edici kontroller tesis edilir.
- Faaliyetlerin yürütülmesi sırasında bilgi sistemleri aracılığıyla edinilen ve saklanan müşteri ve Kurum bilgilerinin gizliliğini sağlamak esastır. Müşteri bilgilerinin, yasalarla yetkili kılınmış merciler dışındaki taraflarla paylaşımına ilişkin uygulama esasları "Kişisel Verileri İşleme, Saklama, Aktarma ve İmha Politikası" ile belirlenir.
- Uygulamaya konulan bilgi sistemlerinin işleyişi, stratejik hedeflere uygunluğu, kontrollerin etkinliği ve yeterliliği, bilgi teknolojilerindeki gelişmeler de göz önüne alınarak düzenli olarak izlenir. Yeni bilgi sistemlerinin Kurumda uygulanmasının, Kurumun risk profile üzerinde yaratacağı etki değerlendirilir. Bu çerçevede, gerek duyulması halinde, bilgi sistemleri işleyişi revize edilir. Yeni edinilmesi planlanan bilgi sistemlerine ait projelerin uygunluğu gözden geçirilip test edilerek Üst Yönetim onayına sunulur.
- Kurumdaki tüm bilgi sistemlerinin zaman bilgisi atomik saatlere göre senkronize edilir.
- Mevcut bilgi sistemlerinin yeterliliği ile yeni teknolojilerin kullanımına yönelik değerlendirmeler yapılır; bunun için gereken kaynak belirlenir.
- Çalışanların bilgi güvenliği ve gizliliği farkındalık düzeylerini artıracak eğitimler verilir.
- Bilgi sistemlerinden kaynaklanan risk düzeyine ilişkin değerlendirmelere ve risk düzeyinin asgari seviyeye indirilmesine yönelik aksiyon planlarının belirlendiği Risk Yönetim Prosedür ve Süreçleri oluşturulur ve güncelliği sağlanır. Bu kapsamda; faaliyetlerin yürütülmesinde uygulanacak kimlik doğrulama ve yetkilendirme süreçleri ile veri gizliliğinin sağlanmasına ilişkin mevcut kontrollerin etkinliği ve yeterliliği değerlendirilir, bilgi sistemlerine ilişkin yılda en az bir defa risk analizi yapılır. Bu analiz bilgi sistemlerinde meydana gelebilecek önemli değişikliklerde tekrarlanır.
- Bilgi güvenliği ihlâline ilişkin olaylar hakkındaki değerlendirmeler yapılırak gerekli tedbirler alınır.
- Bilgi sistemleri ve bilgi güvenliği alanlarındaki güncel gelişmeler ile bunların Kurumda uygulanabilirlikleri ile ilgili değerlendirmeler yapılır.
- Bilgi sistemleri ile bunlara dayalı olarak verilen hizmetlere ilişkin müşteri şikayetleri ve bunların giderilmesine yönelik alınabilecek aksiyonlar belirlenir.
- Bilgi sistemlerinin kullanımıyla ilgili eğitim materyalleri oluşturulur.
- Bilgi sistemleri ve bilgi güvenliğinin yerine getirilmesinde Kurum içinde herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişilere yapılacak sözleşme kapsamında her yıl "Sızma Testi" yaptırılır.
- SPK Mevzuatında belirtilen sürelerde Bilgi Sistemleri Bağımsız Denetimi yaptırılır. Sonuçlar SPK'ya bildirilir.
- Sızma Testi ve Bilgi Sistemleri Bağımsız Denetim çalışmaları sonucu tespit edilen bulgular değerlendirilerek gerekli aksiyonlar planlanır.
- Bilgi sistemleri için alınacak dış hizmetlere ilişkin risk analizi yapılır. Dış hizmetinin alımı süresince Kurumun maruz kalabileceği riskler ile dış hizmet Kuruluşunun sağladığı hizmetin yeterliliği değerlendirilir. Değerlendirme sonuçları, BSGS tarafından Üst Yönetim onayına sunulur. Kurumumuz personeli olmayan üçüncü tarafların, bilgi sistemlerini kullanma ihtiyacı

olması durumunda (destek personeli, vb.) BSGS, bu kişilerin Kurum ile ilgili Bilgi Güvenliği Politika ve Prosedürlerinden haberdar olmalarından sorumludur. Bu amaçla geçici veya sürekli çalışma sözleşmelerinde, sözleşme imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları yapılır. Üçüncü taraflara bilgi sistemine erişim hakkı vermeden önce gerekli güvenlik gereksinimleri tanımlanır ve uygulanır.

Bilgi Sistemleri, bilgi ağı ve/veya kullanıcı bilgisayarı ortamlarının yönetimi dış kaynaklara verilirken, bilgi güvenliği ihtiyaçları ve şartları, bilgi gizliliği her iki taraf arasında kabul edilmiş ve SPK'nun Bilgi Sistemleri Tebliği'nde belirtilen asgari unsurları içeren bir sözleşmede açıkça yer alır. Alt yüklenici Kuruluşlar varsa sözleşmede onları da bağlayıcı hükümler yer alır. Sözleşme öncesinde hazırlanan teknik yeterlilik raporu Üst Yönetime sunulup onaylatılır. Olası riskler için gerekli önlemler alınır. Dış kaynak yoluyla alınan bilgi sistemleri hizmeti kapsamındaki tüm sistem ve süreçlerin Kurumun risk yönetimi, güvenlik ve müşteri gizliliğine ilişkin ilkelerine uygun olması sağlanır. Dış kaynak hizmeti alınan Kuruluşlar, müşteriler ve personel, bilgi sistemleri üzerindeki aktivitelerinin kaydının tutulduğu konusunda bilgilendirilir. Dışarıdan verilen hizmeti takip etmekten öncelikle BSGS sorumludur. Nihai sorumluluk Kurumumuza aittir.

Denetim İz kayıtlarının oluşturulması ve takibi

(1) Kurumumuz, bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis eder. İz kayıtları, işlemin doğasına uygun detay ve içerikte, asgari olarak aşağıdaki bilgileri barındırır:

a) Kaydı oluşturan sistem,

b) Kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi,

c) Kaydı oluşturan işlem ya da olayla birlikte, gerçekleştirilen değişikliğin ne olduğunu gösteren bilgi,

ç) Kaydın ilişkili olduğu tekil kullanıcıyı veya sistemi gösteren bilgi.

(2) Tesis edilecek iz kayıt mekanizmasının, yaşanan bilgi güvenliği olaylarının sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkân tanıyacak nitelikte olması sağlanır.

(3) Bilgi sistemleri dâhilinde gerçekleşen ve faaliyetlerimize ait kayıtlarda değişikliğe sebep olan işlemler ile hassas ya da sır kapsamındaki verilere erişilmesine veya bunların sorgulanmasına, görüntülenmesine, kopyalanmasına, değiştirilmesine yönelik işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesine, değiştirilmesine ve geri alınmasına yönelik aktiviteler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları asgari beş yıl boyunca saklanır.

(4) İz kayıtları güvenilir ortamlarda yedeklenir ve ihtiyaç duyulması halinde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkân verecek şekilde saklanır.

(5) İz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılır. İz kayıtlarına, bilmesi gerektiği kadar prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunması sağlanır. Kullanıcıların kendi faaliyetlerine ilişkin iz kayıtlarına müdahalesi engellenir ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(6) Kurumumuz, iz kayıt sisteminin önceden belirlenmiş ve belirli periyotlarla güncellenen senaryolar çerçevesinde düzenli olarak gözden geçirilmesine, takip edilmesine ve olağan dışı durumlar ile riskli işlemlerin raporlanmasına ilişkin süreçleri tesis eder. Olağan dışı durumlar ile riskli işlemlere yönelik rapor üretilmesi ve rapor sonuçlarının denetim birimlerince takip edilmesi sağlanır.

(7) Kurumumuz, dış hizmet sağlayıcıları tarafından tutulan iz kayıtlarının kendi standartlarına uygunluğunu ve bu iz kayıtlarının kendisi tarafından erişilebilir olmasını temin eder.

Bilgi sistemleri kullanılarak gerçekleştirilen ve Kurum faaliyetlerine ait kayıtlarda değişikliğe neden olan işlemlere ilişkin olarak yeterli detayda ve açıklıkta denetim izleri oluşturulur. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için kullanılan Cryptolog programı üzerinden sisteme ait tüm logların Denetim izi raporu hergün saat 12.00 da E-Posta yoluyla alınarak günlük incelenmektedir. Denetim izlerinin gizliliği, bütünlüğü ve erişebilirliği düzenli olarak gözden geçirilir ve olağandışı durumlar Üst Yönetime raporlanır.

İz kayıtları için Cryptolog programı kullanılmaktadır. Program tarafından İç Denetim/Kontrol Birimi ve BSGS Sorumlusu'na bilgilendirme epostaları gönderilmekte ve günlük takibi yapılmaktadır.

- Tüm çalışanlar aşağıdaki temiz masa kurallarına uymak zorundadır;

  - Çalışma saatleri dışında bilgisayarlar kapalı ya da ekran kilitli şekilde bırakılır. Çalışma saatleri içerisinde başından ayrıldığında mutlaka bilgisayar kilitli bırakılır. Ekran koruyucu 5 dakika içinde devreye girer.
  - Bilgisayarların masaüstlerinde Kurum'a ait gizli bilgiler içeren dokümanlar bulundurulamaz.
  - Bilgisayarlara ait olan şifreler başkası tarafından bilinebilir olmamalı, kesinlikle kâğıt ortamlara yazılı bir şekilde bırakılmamalı, başkalarıyla paylaşılmamalı ve 3 ayda bir değiştirilir.

7. POLİTİKANIN GÜNCELLENMESİ

Bu Politika, en az yılda bir kez gözden geçirilir ve Yönetim Kurulu onayına sunulur. Sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilir ve herhangi bir değişiklik gerekiyorsa revize edilir ve Yönetim Kurulu onayına sunulur. Politika ve revizyonlar tüm çalışanlara duyurulur.

Gözden geçirmelerde;
- Politikanın etkinliği, kaydedilmiş güvenlik ihlal ve hatalarının yapısı, sayısı ve etkisi aracılığıyla gözlemlenir.
- Politikanın güncelliği teknolojik değişimlerin etkisi vasıtasıyla gözlemlenir.
- Politikanın güncelliği değişen personelle birlikte gözden geçirilmeli, işe yeni giren çalışanların katılımı sağlanır.

8. YASAL ZORUNLULUKLAR

- Kurumumuzca uygulanan Bilgi Güvenliği Politikası, ilgili tüm Kanun ve Yönetmelikler ile ilgili SPK Tebliğlerine uyumlu olmak zorundadır.
- Kurumumuzda kullanılmakta olan tüm yazılımların lisans sözleşmeleri olmak zorundadır. Lisanssız ürünlerin Kurum varlıklarında kullanılması yasaktır.
- Herhangi bir bilişim suçu işlediği saptanan personel, yasalarca belirlenen cezai işleme tabidir.
- Bilişim suçları kapsamındaki Kanunlar, hükümler ve gereklilikler takip edilmeli, yasal düzenlemelerde Bilgi Güvenliği Politikasını etkileyen bir değişiklik olduğunda, Politika güncellenir.
- Bilgi güvenliği olayı için kanıt oluşturabilecek herhangi bir veri, değişime uğramayacak ve kanıt özelliğini kaybetmeyecek şekilde saklanır.