EKİZ KİMYA SANAYİ VE TİCARET A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

I. BİRİNCİ BÖLÜM:

A. GİRİŞ:

A.1) Kapsam:

EKİZ KİMYA SANAYİ VE TİCARET A.Ş.'nin stratejik planlarının desteklenmesi, sahip olunan marka değerinin korunması ve ilgili yasal düzenlemelere uyum sağlanması amacıyla izlenmesi gereken bilgi güvenliği kuralları ve prensipleri ile bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanması bu Politika kapsamındadır. Şirket mülkiyetinde olan her türlü bilgi ve bilgi varlığı bu Politika kapsamında olup, Şirket bünyesinde yerine getirilen tüm faaliyetler ve işletilen süreçler bu Politikaya uygun olarak yürütülür.

A.2) Amaçlar:

Bu Politika, Şirketin bilgi ve bilgi varlıklarını koruyacak yapıların kurulmasını, uygulanacak bilgi güvenliği prensiplerinin belirlenmesi ile Şirket Yönetim Kurulu'nun söz konusu çalışma ve prensiplere verdiği destek ve önemi ifade etmeyi amaçlar.

A.3) Dayanak:

Bilgi Güvenliği Politikası, halka açık şirketler için Sermaye Piyasası Kurulu tarafından yürürlüğe konan VII-128.9 Bilgi Sistemleri Yönetimi Tebliği **(Tebliğ),** TS EN ISO 27001 Standardı, Kişisel Verilerin Korunması Kanunu **(KVKK)** ve diğer düzenlemeler dikkate alınarak hazırlanmıştır.

Şirket, Bilgi Güvenliği Yönetim Sistemi süreçlerinin işletilmesi ve sürekliliğinin sağlanması için gereken kontrollerin tesis edilmesini ve gözetimini bu politikaya bağlı alt politikalar, prosedürler ve talimatlar vasıtasıyla sağlar.

A.4) Tanımlar ve Kısaltmalar:

Bilgi: Şirketin görev, sorumluluk ve faaliyetleri çerçevesinde doğrudan kendisi tarafından üretilen veya diğer kurum veya şahıslar tarafından kendisine iletilen ham ya da işlenmiş her türlü veriyi,
Bilgi Güvenliği: Bilgiyi, yetkisiz kişilerin görmesinden, değiştirmesinden, bilgilerin silinmesinden Gizlilik, Bütünlük, Erişilebilirlik kapsamında korunması,
Bilgi Güvenliği Kontrolü: Bilgi veya bilgi varlıklarının sahip olduğu zafiyetin ortadan kaldırılması veya kabul edilebilir seviyeye çekilmesi amacıyla uygulanabilecek bilgi güvenliği önlemlerini,
Bilgi Varlığı: Üretilen bilginin işlenmesi, saklanması, iletilmesi, korunması, sürekliliğinin sağlanması ve yok edilmesi için kullanılan her türlü donanım, yazılım veya iletişim altyapısını,
Bilgi Güvenliği Yönetim Sistemi: Bilgi ve bilgi varlıklarının değişen teknolojik gelişmeler, yasal düzenlemeler, kuruluşun iç/dış iş süreçleri ve tehdit uzayı doğrultusunda olası bilgi güvenliği risklerinin belirlenmesi ve gerekli koruma yöntemlerinin hayata geçirilmesi amacıyla işletilen sistemi,
BGK: Bilgi Güvenliği Komitesini,
BGY: Bilgi Güvenliği Yöneticisini,
BGYS: Bilgi Güvenliği Yönetici Sorumlusunu,
Kullanıcı: Tüm Şirket çalışanlarını ve sözleşmelerle veya diğer vesilelerle kendisine şirket mülkiyetinde veya kullanımında olan bilgi veya bilgi varlıklarına erişim hakkı verilen kişi veya kurumları,
KVKK: 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,
Sektörel /Kurumsal SOME: SOME Tebliği kapsamında Kurul bünyesinde kurulan Siber Olaylara Müdahale Ekibini,
SOME Rehberi: Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanmış en güncel "Kurumsal SOME Kurulum ve Yönetim Rehberi" dokümanını,
SOME Tebliği ve 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği,
USOM: Bilgi Teknolojileri ve İletişim Kurumu bünyesinde yer alan Ulusal Siber Olaylara Müdahale Merkezini,
Tedarikçi: Şirket iş süreçlerinin işletilmesi amacıyla ihtiyaç duyulan hizmet ve/veya kaynakları sunan kişi veya kurumları,
Üst Yönetim: Yönetim kurulu tarafından belirlenen kişi ya da grubu,

İfade eder.

B. ROLLER VE SORUMLULUKLAR:

Bu kısımda Şirketimizin personeli için bilgi güvenliği rolleri ve sorumlulukları tanımlanmaktadır. Bilgi Güvenliği Politikasının hazırlanması, gözden geçirilmesi ve güncellenmesinden, Bilgi Güvenliği Yöneticisi, varsa Kalite Yönetim Temsilcisi ve IT ekibi sorumlulukları da bulunmaktadır.

B.1) Üst Yönetimin Sorumlulukları:

Yönetim Kurulu: Bilgi güvenliği politikası üst yönetim tarafından hazırlanır ve yönetim kurulu tarafından onaylanır. Bilgi güvenliği politikası kapsamında bilgi sistemleri kontrollerinin etkin, yeterli ve uyumlu bir şekilde tesis edilmesi, değerlendirilmesi ve gözetiminden sorumludur. Yönetim Kurulu, politikanın gözetiminden sorumlu "Üst Yönetimi" yetkilendirir. Atanacak yetkiler ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olur.

Üst Yönetim: Bilgi güvenliği politikasının ve bilgi sistemleri stratejisinin uygulanması üst yönetim tarafından gözetilir. Bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Üst yönetim, aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

(1) Bilgi Güvenliği Politikasını onayı ve hazırlanması,
   a) Bilgi ve bilgi varlıklarını koruyacak yapıların kurulması ve güvenlik önlemlerinin uygun düzeye getirilmesi amacıyla hazırlanan "Bilgi Güvenliği Politikası"nın ve tüm sorumluluklarının yılda en az bir kez gözden geçirilmesi ve onaylanarak duyurulmasını sağlar.
   b) Bilgi Güvenliği Politikasının kurum içinde uygulanmasına destek vererek, personele bilgi güvenliği gereksinimleri, riskler ve güncel tehditler konusunda bilgi düzeyini artırmaya yönelik eğitimlerin rol ve sorumluluklarına uygun şekilde yılda en az bir kez verilmesini sağlar.
   c) Bilgi güvenliği ihlallerinin takip edilmesinden ve yılda en az bir kez değerlendirilmesinden sorumludur.
(2) Bilgi Sistemleri Risk Yönetimi sürecinin oluşturulması,
(3) BGYS Sorumlusunun atanması,
   Bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde yeterli teknik bilgiye ve en az 5 yıl tecrübeye sahip bir bilgi güvenliği sorumlusu belirlenir. Bilgi güvenliği sorumlusunun, bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevinin bulunmaması ve üst yönetime bağlı çalışması sağlanır.
(4) Süreklilik Planının hazırlanması,
(5) Yönetsel Rol ve Sorumluluklarının belirlenmesidir.

B.2) Birim Müdürlerinin Sorumlulukları:

(1) Bilgi Güvenliği Politikasını uygulamak,
(2) Kendisine bağlı çalışan personelin erişim yetkilerini onaylamak,
(3) Kendisine bağlı kısımda çalışacak üçüncü taraf bilgi sistemleri kullanıcıların politikalardan haberdar olmasını sağlamak,
(4)Fark ettiği veya kendisine çalışanları aracılığıyla iletilen bilgi sistemleri ile ilgili güvenlik problemlerini BGY Yöneticisine bildirmek,
(5) Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak.

B.3) Bilgi Güvenliği Komitesi'nin (BGK) Sorumlulukları:

(1) Bilgi Güvenliği Sistemlerinin kurulması ve işletilmesi için gerekli kararların alınması ve ihtiyaç duyulan kaynaklara erişilebilirliğinin sağlanarak gerekli süreç ve organizasyon yapısının tesis edilmesi,
(2) Bilgi güvenliğine ilişkin politika ve standartları belirleyerek etkinliğini değerlendirmek amacıyla BGYS performansının izlenmesi,
(3) Bilgi Güvenliği Sistemleri hedeflerinin şirket amaçları ile uyumlu olmasının ve şirket süreçleri ile bütünleştirilmesinin sağlanması,
(4) Şirket bilgi güvenliği stratejilerine yön vermek ve yasalara uyum sağlayarak kontrol mekanizmalarının oluşmasına liderlik edilmesidir.

B.4) Bilgi Güvenliği Yönetici Sorumlusu' nun (BGYS) Sorumlulukları:

(1) BGY Yöneticisini atamak,
(2) Eğitimleri planlamak ve gerçekleşmelerini sağlamak,

(3)BGY Yöneticisinin yapmış olduğu faaliyetleri kontrol etmek, hazırlamış olduğu dokümanları onaylamak ve uygulanmasını sağlamak,
(4) BGY Yöneticisi tarafından hazırlanan Güvenlik Politikalarını gözden geçirerek, üst yönetimin onayına sunmak,
(5)Bilgi sistemleri güvenliğine ilişkin kontrollerin ve gereklerinin yerine getirilmesi ile takibinden sorumlu olmak,
(6)Bilgi sistemleri güvenliğiyle ilgili risklerle bu risklerin yönetimi hususunda üst yönetime rapor sunmak.

B.5) Bilgi Güvenliği Yöneticisinin (BGY) Sorumlulukları:

(1) Bilgi güvenliği ile ilgili konularda bölümler ve dış servis sağlayıcıları arasında koordinasyonu sağlamak,
(2) Güvenlik Politikalarının sahibi olarak, politikaların güncelleştirilmesinden ve uygulanmasından sorumlu olmak,
(3) BGK Komitesinin gündemini belirlemek, alınan kararların uygulanmasını takip etmek,
(4)Kurum genelindeki 27001 kapsamındaki dokümanların Güvenlik Politikası prensiplerine uygun olarak yazılmasını sağlamak,
(5) İş sürekliliği planının işletilmesi, denetlenmesi ve testlerinin yapıldığını kontrol etmek,
(6) Acil durumlarda komite üyeleriyle yakın olarak çalışmak ve bilgi alışverişinde bulunmak,
(7**)** Güvenlik zaafları ve olaylarının nedenlerini araştırmak; gerektiği zamanlarda delilleri saklamak ve raporlar, önlemler ve iyileştirme önerilerinde bulunmaktan sorumludur.

B.6) Kurum Personelinin Sorumlulukları:

(1) Bilgi Güvenliği Politikaları kurallarına uymak,
(2) Çalışan personeller için hazırlanmış roller ve sorumluluklarla ilgili dokümanlarında belirtilen görevleri yerine getirmek,
(3) Sahibi olduğu bilgi varlığını korumak ve gerektiğinde güncellemelerde bulunmak, herhangi bir hata/arıza/olay olduğunda ilgili kişilere haber vermek,
(4) Acil durum komite üyeleriyle yakın olarak çalışmak ve bilgi alışverişinde bulunmak,
(5) Bilgi güvenliği için kullanılan donanım ve yazılım kullanım talimatlarına uymak, alınan eğitimleri uygulamak ve yöntemler geliştirmek.
(6) İşleri gerçekleştirmek için kendisine verilmiş olan ayrıcalıklı kullanıcı kimlikleri var ise bu kimliği ve hakları sadece bu işi yaparken kullanmak,
(7) Herhangi bir bilgi güvenliği olayını fark ettiğinde, zaman geçirmeden BGY Yöneticisine bilgi vermek ve yardım masası ortamına kayıt girmek.

II. İKİNCİ BÖLÜM:

A. VARLIK YÖNETİMİ:

(1) Şirket, kendisi için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurları içeren sahip olduğu bilgi varlıklarının "Envanter"i oluşturulur ve güncelliğini sağlanır.
(2) Bilgi varlıklarının güvenlik sınıfının belirlenmesi için bir "Kılavuz" oluşturulur ve bu Kılavuz Üst Yönetimce onaylanır.
(3) Taşınabilir cihaz ve ortamlar, içerdiği bilgilerin güvenlik sınıfına göre kaybolma, hırsızlık ve kopyalama gibi risklere karşı korunur. Güvenlik sınıfı yüksek bilgileri veya bu bilgilere erişim sağlayan yazılımları barındıran taşınabilir cihaz ve ortamlar izinsiz kurum dışına çıkarılmaz.
(4) Bilgi varlıklarına ilişkin uygun kullanım Prosedürleri geliştirilir, yazılı hale getirilir, üst yönetim tarafından onaylanır ve ilgili personele imza karşılığı duyurulur.
(5) Kullanımdan kaldırılan donanımsal varlıklara güvenli silme veya imha işlemleri uygulanır ve kayıt altına alınır. Kullanımdan kaldırılan yazılım ve uygulamalara erişimler engellenir ve gerekirse bu yazılım ve uygulamalar arşivlenerek sistemden silinir.
(6) Bilgi varlıklarının sınıflandırılmasından ve bu sınıflandırmanın belirli zamanlarda gözden geçirilmesinden BGY Yöneticisi sorumludur.

B. RİSK YÖNETİMİ:

(1) Şirket, bilgi sistemlerine ilişkin riskleri belirlemek, ölçmek, izlemek, işlemek ve raporlamak üzere risk yönetimi süreç ve prosedürlerini tesis eder ve güncelliğini sağlar.
(2) Bilgi sistemlerine ilişkin risk analizi, risk işleme ve gözetim süreçleri işletilir. Risk analizi yılda en az bir defa yapılır.
(3) Bilgi sistemlerinin güvenlik açıklarına ve bilgi güvenliği tehditlerine ilişkin bilgi zamanında elde edilir, değerlendirilir ve belirlenen riske karşı uygun tedbirler alınır.
(4) Risk yönetiminde; İyileştirici faaliyetlerin gerekli iş gücü, kaynak ve zaman bilgisiyle kayıt altına alınarak, takibi sağlanır.
(5) İyileştirici faaliyetler ve risk analizi üst yönetime onaylatılır.
(6) Bilgi sistemleri stratejisine ve mevzuata aykırılık teşkil etmeyecek şekilde, iş ve bilgi güvenliği hedefleriyle uyumlu risk kabul kriterleri ile risk işleme seçeneklerinin belirlenerek üst yönetime onaylatılır.

C. ERİŞİM YÖNETİMİ VE DENETİMİ:

C.1) Kullanıcı Erişimi Yönetimi:

(1) Şirket, Bilgi sistemlerine erişim ve uygulamaların kullanımı için uygun erişim kontrollerini tesis eder. Kullanıcılara verilecek yetki düzeyinin belirlenmesinde görev ve sorumluluklar göz önünde bulundurularak gerekli olacak en düşük yetki atanması ve en kısıtlı erişim hakkı verilmesi sağlanır.
(2) Kullanıcıların erişim hakları ve yetkiler her değişiklikten sonra ve yılda en az bir defa ilgili bilgi varlığının sorumlusu tarafından gözden geçirilir.
(3) Kullanıcılara hesap açma, yetkilendirme ve erişim haklarına yönelik diğer işlemler görevler ayrılığı ilkesi kapsamında onay sürecine bağlanır. Erişim haklarına ilişkin gerçekleştirilen tüm işlemlerin denetim izleri tutulur ve düzenli olarak gözden geçirilir.
(4) Gerekli bir iş gereksinimi olmayan yetkiler iptal edilir. İşten ayrılan personel için gerekli hesap kapatma, birim değiştiren kullanıcıların ise erişim haklarının düzenlemesi işlemleri yapılır.
(5) Kullanıcıların sunuculara olan yetkisiz erişim denemeleri ile hak sahibi personelin erişimleri güvenlik yazılımlarıyla kontrol edilerek, gerektiği takdirde rapor edilir.
(6) Bilgi sistemlerinde ortak veya varsayılan hesapların kullanılması -zorunlu olduğu durumlar haricinde- engellenir, kullanılması gereken durumlarda bu hesapları kullananlara sorumluluk atamaya yönelik kontroller tesis edilir ve bu hesaplarca gerçekleştirilen işlemlerin denetim izi tutulur.
(7) Bilgi sistemleri kullanıcılarına zorunlu olmadıkça yerel yönetici hakları verilmez. Yapılacak işin gerektirdiği durumlarda ise ancak BGY Yöneticisinin onayı ile söz konusu haklar verilir.
(8) Bilgi sistemlerinde ayrıcalıklı yetkileri gerektirecek iş ve işlemler için ayrı hesaplar açılır. Bu hesaplarca gerçekleştirilen işlemlerin denetim izni tutulur.

C.2) İşletim Sistemi Erişimi Denetimi:

(1)Başarısız oturum girişimleri güvenlik yazılımları tarafından kaydedilip, gerektiğinde incelenmek üzere saklanmaktadır.
(2) BGYS Sorumlusu tarafından onaylı olmayan lisanssız yazılımlar kullanıcı bilgisayarlarına yüklenmez.

C.3) Uygulama Erişimi Denetimi:

(1) Uygulama sistemlerinin kullanıcıları, erişim isteklerini ilgili formu doldurup bağlı bulundukları birim müdürünün imzalı onayı ile BGY Yöneticisine ileterek erişim yetkisi talebinde bulunurlar ve sadece onay verilen kısma ulaşabilirler.
(2) Uygulamalara erişimler, merkezi kayıt izleme yazılımına yönlendirilerek, saklanır.

C.4) Dışarıdan Sisteme Erişim Denetimi:

(1) Dış ağlardan Kurum iç ağına doğru yapılan erişimler denetlenir.
(2) Saldırı tespit ve önleme sistemi, antivirüs ve kötü niyetli kod engelleme sistemleri daima aktif durumda tutulur.

C.5) Uzaktan Erişim Denetimi:

(1) Uzaktan erişim yetkilendirmeleri BGYS Sorumlusunun onayı alınarak yapılır.
(2) Uzaktan erişim hizmetinde kimlik doğrulama kullanılır. Ağ altyapı cihazlarına fiziksel erişim ile veya uzaktan erişim (SSL, SSH üzerinden) güvenli kanallar üzerinden bağlantıları için çok faktörlü kimlik kontrolü yapılır.

(3) Uzaktan erişim, yalnızca uygulamaları ve işletim sistemleri güncel cihazlardan yapılır. Uzaktan erişime ilişkin denetim izleri tutulur.
(4) Uzaktan erişim bağlantıları, güncel ve güvenilir kararlı sürüme sahip iletişim protokolleri ile sağlanır. Uzaktan erişim oturumları, tanımlanan süre boyunca işlem yapılmadığında otomatik olarak sonlandırılır ve yeniden erişim sağlanması gerektiğinde kimlik doğrulama tekrarlanır.
(5) Mobil cihazların kurumsal ağa erişimine ilişkin risklere yönelik güvenlik önlemleri alınır ve uygulanır.

C.6) Ağ Erişim Güvenliği ve Denetimi:

(1) Kurumsal ağın tüm alt ağları, güvenlik cihazlarını, erişim noktalarını ve bağlantı yollarını içerecek şekilde yazılı hale getirilir, güncel tutulur ve güvenli saklanır.
(2) Kurum ağı içerisinde kullanıcılar sadece gerekli olan sunuculara erişimleri bulunmakla birlikte sadece gerekli olan portlara erişimleri olmalıdır.
(3) Kurum ağı içerisinde ayrı VLAN yapıları olması zorunludur. Kritik sistemler ve kullanıcı bilgisayarları farklı VLAN üzerinde bulunmalıdır.
(4) İç ağın farklı güvenlik gereksinimlerine sahip alt bölümleri birbirinden ayrılarak denetimli geçişi temin eden kontroller tesis edilir. Bu kapsamda asgari olarak; istemciler, sunucular ve yönetimsel işlemler için ayrı alt ağlar oluşturulur. Kablolu ve kablosuz ağlar birbirinden ayrılır.
(5) Ağ altyapı elemanlarında kimlik doğrulama açık olmalı ve yetkisiz erişimler engellenmelidir. Anahtarlama cihazında kimlik doğrulama; cihaza yönetimsel veya denetimsel erişim söz konusu olduğu zaman kişinin doğru kişi olup olmadığının kontrolü gerekir.
(6) İletişim altyapıları dinlemeye ve fiziksel hasarlara karşı korunur. İnternet üzerinden erişimlerde uçtan uca güvenli iletişim teknolojileri kullanılır.
(7) Bilgi güvenliği gereksinimlerine ve yasal gerekliliklere uygun olmayan internet sitelerine erişim ile ağ erişimleri beyaz liste veya kara liste yapıları kullanılarak sınırlandırılır ve güvenilmeyen bağlantılar engellenir.
(8) Kablosuz ağlarda güçlü şifreleme protokolleri kullanılır. Kablosuz ağlar için kimlik doğrulama ve erişim kontrolleri uygulanır. Kimlik doğrulama işlemleri, güvenilir ve güncel protokollerle gerçekleştirilir. Misafir ağları kurumsal ağlardan ayrı tutulur, misafir ağı kullanıcılarına geçici ve kısıtlı erişim hakkı verilir.
(9) İç kaynak yoluyla veya dışarıdan hizmet olarak alınan her türlü ağ hizmetinin güvenlik kriterleri, hizmet düzeyleri ve yönetim gereksinimleri tanımlanır ve hizmet anlaşmalarına dâhil edilir.
(10) İnternet üzerinden sunulan hizmetler hizmet dışı bırakma saldırılarına karşı korunur.
(11) Kurumsal ağın dış ağlarla olan iletişiminde dış ağlardan gelebilecek tehditler için sürekli gözetim altında tutulan güvenlik duvarı ile ağdaki anormal aktiviteleri ve saldırı girişimlerini tespit etmek ve engellemek için günün teknolojisine uygun çözümler kullanılır. Hassas veri içeren bilgi sistemlerine, internet üzerinden doğrudan erişim engellenir.

C.7) Genel Güvenlik Denetimleri:

(1) Kullanıcılar, kullanmadıkları zamanlarda ekranlarının izinsiz kişilerce görülmesini engellemek için işletim sisteminin ekran kilitlenmesi özelliğini etkin hale getirmek gibi gerekli önlemleri almalıdırlar. İlkenin tam olarak uygulanması için, merkezi olarak buna uygun kurallar bütün kullanıcı bilgisayarları ve sunuculara dağıtılmalıdır.
(2) Kurum kullanıcıları, kendilerine verilmiş olan kullanıcı adı ve şifrelerinin sadece kendileri tarafından kullanılması ilkesini koruma sorumluluğuna uymalıdırlar. Bu ilkenin ihlali durumunda kullanıcı sorumlu olacaktır.
(3) Varlık sınıflandırmasında hassas bilgi olduğu belirlenen dokümanların kâğıt baskılarının erişim yetkisi olmayan kişilerce erişimini engellemek amacıyla kurum personeli tarafından temiz masa politikası uygulanmadır. Temiz masa politikası, önemli dokümanların diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmecelerde saklanmasıdır. Bu şekilde masa üstlerinde hassas bilgilerin bulunmayacağı garanti altına alınmalıdır.
(4) Kullanıcıların çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmaları ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamaları gerekmektedir.
(5) Kurum cihazları güvenlik açısından gerekli görüldüğünde merkezi olarak kontrol edilebilecektir.

III. ÜÇÜNCÜ BÖLÜM:

A. BİLGİ GÜVENLİĞİ'NİN KURUMSAL ALT YAPISI:

A.1) Bilgi Güvenliği Altyapısı:

(1) Bilgi güvenliği ile ilgili tüm faaliyetlerden BGY Yöneticisi sorumludur.
(2) ISO 27001 Bilgi Güvenliğinde alınan kararları birimlerde bulunan diğer personele aktarılması görevini BGYS Koordinasyon Ekibi üstlenir. Bu koordinasyon; BG Komitesi, BGYS Sorumlusu ve BGY Yöneticisi, görevler tablosunda yer alan çalışanlardan oluşmaktadır. Bu toplantılara BGY Yöneticisi ve BGYS Sorumlusu katılmak zorundadır. Diğer personel gerekli olan durumlarda toplantılara katılmalıdır. BGY Yöneticisi, BGYS Koordinasyon Ekibinin toplanmasından sorumludur.
(3) BGYS Koordinasyon ekibi senede en az bir kez toplanmalıdır. Önemli bir güvenlik olayı olduğu zamanda da olağanüstü toplanmalı ve gündem aşağıdaki maddeleri içermelidir.
a) Bilgi güvenliği politikalarının ve sorumlulukların gözden geçirilmesi,
b) Büyük tehditlere karşı varlıklardaki önemli değişikliklerin değerlendirilmesi,
c) Bilgi güvenliği olaylarının ve hatalarının gözden geçirilmesi,
d) Bilgi güvenliği için önceliklerin gözden geçirilmesi.
(4) BGYS Sorumlusu, yukarıda belirtilen gündeme konu ekleyebilir, gündemden konu çıkarabilir gündem ve toplantı tarihini bir başka tarihe erteleyebilir.
(5) BGK Komitesi ise, BGYS Sorumlusu ya da BGY Yöneticisi başkanlığında gerekli gördüğü zamanlarda ya da belirli aralıklarla toplanır.

A.2) Müşterilerin Bilgilendirilmesi:

(1) Kurum tarafından elektronik ortamda sunulan hizmetlerden yararlanacak müşteriler; ispat yükü Şirket'in sorumluluğunda olmak üzere sunulan hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir.
(2) Bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterilerin yaşayabileceği sorunların takip edilebileceği ve müşterilerin şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmalar oluşturulur. Şikâyet ve uyarılar değerlendirilerek aksaklıkları giderici çalışmalar yapılır.

A.3) Dışarıdan Hizmet Alımı:

(1) Üst yönetim, dışarıdan alınan kritik hizmetlerin erişilebilirliğini, performansını, kalitesini, bu hizmet kapsamında gerçekleşen güvenlik ihlalleri ile dış kaynak yoluyla hizmet sağlayan kuruluşun güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu yakından takip etmek için yeterli bilgi ve tecrübeye sahip sorumluları belirler. Bu sorumlular, yılda en az bir defa olmak üzere bu maddede sayılan hususları içeren bir değerlendirme raporu hazırlar ve üst yönetime sunar.
(2) Dışarıdan hizmet alımına ilişkin koşul, kapsam ve her türlü diğer tanımlama, dış hizmeti sağlayan kuruluşça da imzalanmış olacak şekilde Hizmet Sözleşmelerine bağlanır. Kritik olmayan hizmetler, standart sözleşmeler ile alınabilir ve bu durumun gerekçesi yazılı hale getirilir.
(3) Dışarıdan hizmet sağlayan kuruluşlara verilen erişim hakları özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır, gerekiyorsa ek kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim türü, erişilecek verinin hassasiyeti ile erişimin bilgi güvenliği üzerindeki etkileri dikkate alınır. Erişim hakları, işin gerektirdiği en az yetkiyi içerir ve gerekirse zamana bağlı olarak tanımlanır. Alınan hizmetin sonlanması durumunda ilgili tüm erişim hakları iptal edilir.
(4) Faaliyetlerinin tamamı veya bir bölümü için bulut hizmeti kullanabilir. Platformlar, bulut hizmet sağlayıcısının yurt içinde temsilciliğinin bulunması koşulu ile müşteri emirlerinin eşleştiği ortamlar için tüm kayıtlar gün sonunda yurt içindeki sistemlere aktarılmak şartıyla yurt dışı bulut hizmeti kullanabilir. Bulut hizmeti alımı, kullanımı ve yönetimi, dışarıdan hizmet alımı olarak değerlendirilir.
(5) Dışarıdan alınan yazılım, donanım, işletim sistemi veya bu bileşenlerin bir ya da birkaçını barındıran cihaz/sistemlerin, mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıklarını barındırmadığına yönelik taahhütname; dağıtıcı, tedarikçi veya üreticiden alınır.

A.4) Üçüncü Şahıslarla Bilgi Değişimi:

(1) Kurum personeli olmayan üçüncü tarafların, bilgi sistemlerini kullanma ihtiyacı olması durumunda (ör: kurum dışı bakım onarım personeli vb.) BGY Yöneticisi, bu kişilerin kurum ile ilgili bilgi güvenliği politikalarından haberdar olmalarından sorumludur. Bu amaçla geçici ya da sürekli çalışma sözleşmelerinde sözleşme

imzalanmadan önce kararlaştırılmış ve onaylanmış güvenlik anlaşmaları yapılmalıdır. Bu kapsamda yapılan çalışmalar yazılı hale getirilir ve veri aktarımlarına ilişkin denetim izi tutulur.
(2) Gerektiği takdirde bakım personelinin politikaya uyması için süre tahsis edilmelidir.
(3) Gizlilik Sözleşmesi ve Bilgi Güvenliliği sözleşmesi imzalanacak firma ve kişileri, acil olduğu durumlarda BGY Yöneticisi normal koşullarda ise BGK Komitesi belirler.

A.5) Kayıt Mekanizmasının Oluşturulması, Verilerin Bütünlüğü:

(1) Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır. Denetim izlerinin bütünlüğü düzenli olarak gözden geçirilir ve olağan dışı durumlar üst yönetime raporlanır.
(2) Denetim izlerinin yeterli güvenlik düzeyine sahip ortamlarda korunması ve yedeklerinin alınması suretiyle, yaşanması muhtemel olumsuzluklar sonrasında da öngörülen süre için erişilebilir olmaları temin edilir. Bunun yanı sıra, denetim izlerinin alınması ve saklanmasında kullanılan araç veya yöntemler gözetim altında tutulur. Denetim izi mekanizmasında bir aksaklık yaşandığında ilgili kişilerin otomatik olarak uyarılması sağlanır. Denetim izleri asgari 5 yıl saklanır.
(3) Kullanıcılar, bilgi sistemleri üzerindeki aktivitelerinin kaydının tutulduğu konusunda bilgilendirilir.
(4) Denetim izleri sürekli gözetim altında tutulur. Olağan dışı durumlar için otomatik uyarı mekanizması kurulur ve ilgililere bildirim yapılır. Bu bildirimlerin her biri üzerinde inceleme yapılır ve sonuçlar kayıt altına alınır.
(5) Dışarıdan alınan hizmetler için de bu madde kapsamında denetim izi tutulması ve Kurum tarafından erişilebilmesi sağlanır.
(6) Denetim izleri merkezi bir kayıt yönetim sistemi aracılığıyla izlenir ve analiz edilir. Olası güvenlik olaylarının erken tespiti için korelasyon kuralları tanımlanır ve uyarı mekanizmaları oluşturulur.
(7) Kritik faaliyetlerin gerçekleştiği bilgi sistemlerinin yöneticileri ile bu sistemlere ilişkin denetim izlerini yöneten kişiler ayrıştırılır.
(8) Şirket bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli önlemleri alır. Bütünlüğü sağlamaya yönelik önlemler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde tesis edilir. Bilgi sistemlerine ilişkin dışarıdan hizmet alınan kuruluşlar nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilir.
(9) Kritik işlemler, kayıtlar ve verilerde meydana gelebilecek bozulmaları saptayacak ve zamanında gerekli bildirimleri yapacak teknikler kullanılır.

B. BİLGİ SİSTEMLERİ'NİN FİZİKSEL VE ÇEVRESEL GÜVENLİĞİ:

B.1) Personel Bilgi Güvenliği:

(1) Tüm çalışanlar, kurumun bilgi güvenliği politikalarına uymakla yükümlüdürler. Kullanıcılar, politikalara uygun olmayan davranışları sonucu meydana gelebilecek bilgi sistemleri olaylarından sorumlu olacaklardır.
(2) Kurum çalışanları, kurum personeli olduğu sürece ve kurumdan ayrılmaları (emeklilik, istifa, vs.) durumlarında kurum bilgilerini gizlilik prensibine uygun olarak korumaktan sorumludur.
(3) İşten ayrılan veya kurum içinde görev değişikliği olan personel için kullanıcı hesaplarının silinmesi, erişim yetkilerinin değiştirilmesi gibi gerekli kontroller hemen yapılmalıdır.
(4) Üçüncü şahıslar da dâhil olmak üzere, Şirketin bilgi sistemlerini kullanması gereken her personel için varlık ve kaynakların doğru kullanımı da dâhil olmak üzere uygun güvenlik politikaları ve prosedürleri konusunda gerekli taahhütnameler hazırlanmalı ve ilgili personele imzalatılmalıdır.
(5) Kullanıcı adı açılmış tüm kurum personeline ve her yeni personel alımı sonrasında yeni personele farkındalık eğitimi verilmelidir.

B.2) Güvenlik Korumalı Bölgeler:

(1) Kritik veya hassas iş faaliyetlerini desteklediği belirlenen tüm bilgi teknolojisi araçları, fiziksel erişim kontrolü gerektiren alanlarda bulunmalıdır.
(2) Tüm personelin giriş yetkisi/izni olmayan alanlara girmemeleri gerektiği unutturulmamalıdır.
(3) Güvenli alanlara alınacak ziyaretçilere atanmış kurum personeli sürekli eşlik etmeli ve ziyaretleri süresince güvenli bölgelerde yalnız bırakılmamalarına dikkat edilmelidir.
(4) İzin verilmediği sürece güvenli alanlarda fotoğraf çekmek, görüntü almak ve ses kaydetmek yasaktır.
(5) Güvenli alanlara izinli personel dışındaki tüm kişilerin giriş ve çıkış saatleri ziyaret defterine kaydedilmelidir.
(6) Destekleyici altyapı hizmetlerinin, uygun çalışma koşullarının dışına çıkılması halinde, alarm üretmesi ve ilgilileri bilgilendirmesi sağlanır.
(7) İklimlendirme kontrolü ile uygun ortam koşullarında çalışma sağlanarak, yangın, sel, deprem, patlama ve diğer doğal ya da insan kaynaklı felaketlerden kaynaklanan hasara karşı fiziksel koruma tasarlanır ve uygulanır.

B.3) Donanımsal Güvenlik:

(1) Bilgi teknolojisi araçlarının, herhangi bir elektrik kesintisinde çalışmalarına devam etmeleri için kullanılan UPS, jeneratör gibi güç kaynakları yılda en az iki defa olmak üzere periyodik olarak üreticinin talimatlarına uygun biçimde kontrol edilmelidir.
(2) Tüm donanımların, elverişliliği ve güvenilirliği garanti etmek amacıyla üretici firmanın talimatlarına uygun olarak, düzenli periyodlarla bakımları yapılmalıdır. Bakım ve onarım hizmetlerini gerçekleştirecek kişilere çalışma öncesi gizlilik sözleşmesi imzalatılır
(3) Güç kaynaklarının sağlıklı şekilde çalışabilmesi için gerekli tedariklerin önceden planlanarak tedarik edilmesi sağlanmalıdır.
(4) Dizüstü bilgisayar, belge, CD ve taşınabilir bellek gibi taşınabilir kurum varlıklarının korunması için gerekli önlemlerin alınmasından envanter sisteminde varlık sahibi olarak kaydedilmiş kişi sorumludur. Herhangi bir kaybolma veya çalınma durumunda da hasarı karşılayacak kişi varlık sahibidir.
(5) Kurum dışına çıkarılabilen varlıklar kurum dışında çalışırken gizlilik prensipleri ve varlık sınıflandırmaları göz önünde bulundurulmalıdır.
(6) Personel, adlarına kayıtlı taşınabilir cihazların korunmasından kurum dışına çıkıldığı durumlarda da sorumludurlar. Ayrıca kendisine ait varlıkları (şahsi dizüstü bilgisayar, tablet vb) BGY Yöneticisinden habersiz kurum sistemlerine sokamaz.
(7) Personel, önemli varlıkların bulunduğu güvenli alanlarda sigara içmemeli, yiyecek ve içecekle güvenli alana girmemelidir.

C. BİLGİ SİSTEMLERİ'NİN İŞLETİM GÜVENLİĞİ:

C.1) İşletim Prosedürleri: Kurum içi donanım ve uygulamaların işletim prosedürleri hazırlanır. Tüm kritik işletim prosedürleri yazılı olarak bulunur ve ihtiyaç duyulduğunda sürekli erişilebilen ortamlarda yayınlanır. Yazılı prosedürler ihtiyaç duyulduğunda BGY Yöneticisi tarafından hazırlanır ve BGYS Sorumlusu tarafından onaylanarak geçerlilik kazanır. Onaylı olmayan işletim prosedürleri geçersiz sayılır.

C.2) Olay Yönetimi: Bilgi güvenliği ihlal olayı olarak değerlendirilen her durum için düzeltici önleyici faaliyet formu oluşturulur ve yardım masası ortamına kayıt açılır.

C.3) Bilgi Ortamı Yönetimi ve Güvenliği:

(1) İşlemlerin, prosedürlerin, veri yapılarının, yetkilendirme işlemleri gibi hassas bilgilerin bulunduğu sistem dokümantasyonu, yetkisiz kişilerin erişimini engellemek amacıyla güvenli ortamlarda bulundurulmalı, gerekli olmadığı sürece bilgi varlıkları yetkisiz kişilerle paylaşılmamalıdır.
(2) Bilgi varlıklarının dağıtımı veya nakli sırasında uygun güvenlik tedbirlerinin alınmasına dikkat edilmeli, taşınabilir ortamdaki bilgi artık kullanılmayacaksa silinmelidir.
(3) Web sitesi, çevresel bilgi sistemi ve diğer yollarla İnternet üzerinde bulunan halka açık kurum bilgilerinin izinsiz olarak değiştirilmesine, eklenmesine veya silinmesine karşı gerekli koruma önlemleri alınmalı ve yetkilendirmeler yapılmalıdır.
(4) Dışarıdan yardım alınacak üçüncü şahıs firmaları ve dış kaynaklı çalışma personeline gerektiği takdirde geçici yetkileri bulunan kullanıcı hesapları tanımlanmalıdır. Bu hesaplar çalışma biter bitmez devreden çıkarılmalıdır.
(5) Güvenlik açıklarına ilişkin yayınlanan yamaların uygulanması değerlendirilerek, uygulanmasına karar verilen yamalarla ilgili olarak BGYS Sorumlusuna düzenli rapor verilir.

D. SİSTEM PLANLAMASI VE GENİŞLETMESİ:

(1) Kritik bilgi sistemleri, hizmet seviyelerine uygun performansta çalışması için sürekli gözetim altında tutulur, sistemlerin her biri için eşik değerler belirlenir ve bu değerlerin aşılması durumunda ilgili kişilere otomatik bildirim gönderilmesi sağlanır.
(2) Varlık envanterinde kaydı bulunan her türlü varlık faaliyetlerdeki olası büyüme, kullanıcı sayısındaki artış ve benzeri durumlar dikkate alınarak bilgi sistemlerinin beklenen performans düzeyinde çalışabilmesi için kapasite planlaması yapılır. Beklenen performans değerinin altına düşüldüğü durumlarda kök sebep araştırılır ve gerekli iyileştirici faaliyetler gerçekleştirilir.

IV. DÖRDÜNCÜ BÖLÜM:

A. TEKNİK GÜVENLİK İLKELERİ:

A.1) Bilgi Güvenliği İhlali Önlemleri:

(1) Kurum, bünyesinde gerçekleşen her türlü bilgi güvenliği ihlalinin veya bilgi sistemlerine ilişkin tespit edilen güvenlik açıklarının yönetilmesini sağlayacak kontrolleri tesis eder ve bu kapsamda tüm personel, rol ve sorumlulukları hakkında bilgilendirilir. Gerçekleşen ihlal veya tespit edilen güvenlik açığı mümkün olan en kısa sürede kayda alınır ve gerekli işlemler yapılır.
(2) Bilgi güvenliği ihlal olaylarının veya güvenlik açıklarının değerlendirilmesi için kriterler belirlenir. Bu kriterler asgari olarak kritik operasyonların ve hizmetlerin olası kesinti süresi, veri sızıntısı kapsamında çalınan kayıt veya etkilenen hesap sayısı, etkilenen kullanıcı sayısı, kesinti süresince ve ileriye dönük toplam gelir kaybı, ihlal edilen hizmet seviyesi anlaşmalarının oranı ölçütlerini içerir ve bu süreç yazılı hale getirilir.
(3) Bilgi güvenliği ihlal olaylarına müdahale planı hazırlanır ve üst yönetim tarafından onaylanır.
(4)Yaşanan olayın, kritik operasyonları kesintiye uğratacak veya veri sızıntısıyla sonuçlanacak potansiyelde belirlenmesi durumunda derhal Kurul, müşteriler ve ilgili diğer kurumlar bilgilendirilir.
(5) Olay sonrası, olaya ilişkin alınan kararlar, olayın etkilediği bilgi sistemleri ve iş süreçleri, olaya cevaben gerçekleştirilen tüm işlemler, olayın kök sebebi, görev alan kişiler, harcanan zaman, maliyet ve işgücü miktarı kayda alınarak siber olay müdahale raporu hazırlanır ve üst yönetime iletilir. Olaydan kritik sistemler veya hassas verilerin etkilenmesi durumunda hazırlanan rapor derhal Kurula iletilir.
(6) Olay müdahale süreciyle ilgili personelin yetkinlik, deneyim ve bilgisinin eğitim programları ile artırılması sağlanır.
(7) Sektörel SOME tarafından, Kurumsal SOME kurulmasına karar verilirse, bilgi güvenliği ihlallerine ilişkin gerçekleştirilen faaliyetlere yönelik yıllık olarak SOME Rehberinde belirtilen Kurumsal SOME Faaliyet Raporu düzenlenir, üst yönetime raporlanır. Kurumsal SOME üyelerinin iletişim bilgileri USOM tarafından belirlenen yöntem ile USOM'a bildirilir ve güncelliği sağlanır.

A.2) Kimlik Yönetimi İlkeleri:

(1) Bilgi sistemleri üzerinden gerçekleşen işlemler için, bilgi varlığının güvenlik sınıfına uygun kimlik doğrulama yöntemleri belirlenir ve uygulanır.
(2) Kimlik doğrulama yöntemi, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde uygulanır.
(3) Kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek gerekli önlemler alınır.

A.3) Veri Gizliliği İlkeleri:

(1) Kurum, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemleri alır.
(2) Bilgi sistemleri aracılığıyla edindiği veya sakladığı kişisel verilerin gizliliğini sağlamaya yönelik kontrolleri tesis eder ve bunların gerektirdiği önlemleri alır.
(3) Saklama süresi sona eren verilerin bulundukları tüm ortamlardan güvenli ve geri döndürülemez şekilde silinmesi sağlanır ve yapılan işlemler kaydedilir.
(4) Kurum, kişisel verilerin korunması ve işlenmesine yönelik gerekli tedbirleri alır. Bu maddede yer almayan durumlarda 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili diğer mevzuat hükümleri uygulanır.

A.4) Virüs ve Zararlı Yazılımlara Karşı Korunma İlkeleri:

(1) Kurum, genelinde kötü niyetli yazılımlara karşı gerekli korunma önlemleri alınmakta ve altyapı yeni tehditlere karşı sürekli olarak gözden geçirilip güncellenmektedir.
(2) Kurum bilgisayar ağına bağlı olarak çalışan bilgisayarlara anti-virüs programının yüklenmesi zorunludur. Eğer personelin bilgisayarında bu yazılım yok ise ya da güncelliğini yitirmiş ise bunu ilgili birime bildirmekle yükümlüdür.
(3) Anti virüs programı, kullanıcıların kişisel bilgisayarına önceden tanımlanmış standart yapılandırma değiştirilemeyecek şekilde kurulur. Bu yapılandırmanın, bilgisayarı kullanan personel tarafından değiştirilmesi yasaktır.
(4) Bilgisayar Virüsleri karmaşık ve gelişmiş olabileceğinden, personelin bunları uzman yardımı olmadan, yok etmeye çalışmaması gerekir. Eğer personel virüsten şüphelenirse, hemen ilgili bilgisayarı kullanmayı bırakmalı, tüm iletişim ağlarıyla bağlantıyı kesmeli ve ilgili birime haber vermelidir. Eğer şüphelenilen virüs, bilgilere ve yazılıma zarar vermeye başlarsa, personel hemen bilgisayarı kapatmalıdır ve müdahale yapılmasını beklemelidir.

(5) Masaüstü, dizüstü ve sunucu sistemler, taşınabilir bir ortam veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılır ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanır.
(6) BGY Yöneticisi virüs istilası ve sistem arızaları gibi acil durumları kontrol altına alabilmek için özel kullanıcı dosyalarını inceleme yetkisine sahiptir. Buna dâhil olan kullanıcı(lar) bilgilendirilme yapıldıktan sonra incelenecektir.
(7) Özel yazılımlarla paylaşım alanlarına yapılan bağlantılar kullanıcı adı ve şifre korumalı olmalı paylaşım alanı üzerindeki her türlü hareket kayıt altına alınmalıdır. Paylaşım alanına özel erişimler için destek ortamına kayıt açılmalı ve BGY Yöneticisi onayı alınmalıdır.
(8) Gerekli görülen ek önlemler BGK Komitesi toplantısında tartışıldıktan ve gerekli testleri yapıldıktan sonra sisteme entegre edilmelidir. Ancak, kullanıcılar önlemlere güvenerek sistemi savunmasız bırakacak biçimde hareket etmemelidir.

A.5) Kullanıcı Bilgi Güvenliği Eğitimi:

(1) Kurum personeline asgari olarak bilgi güvenliği politikasından, kullanıcıların uyması gereken kurallardan, güvenlik olayı ihlallerinde nelerin yapılması gerektiğinden, bahsedilen eğitimler verilir. Bu eğitimlerde bilgi güvenliği gereksinimleri, riskler ve güncel tehditler konusunda bilgi düzeyini artırmaya yönelik eğitimlerin rol ve sorumluluklarına uygun şekilde yılda en az bir kez verilmesi amaçlanır.
(2) Yazılım geliştirme süreçlerinde görev alan personele güvenli yazılım geliştirme konusunda kullanmakta oldukları programlar ve genel sistem yapısı ile ilgili bilgilerden eğitim, olay müdahale süreciyle ilgili personelin ise yetkinlik, deneyim ve bilgisinin eğitim programları ile artırılması için eğitim alması sağlanır.
(3) Yapılacak her türlü değişiklik için; değişikliğin sebebini, kapsamını, etkisini, içerdiği riskleri, beklenen faydasını, değişikliği yapacak kişileri, maliyetini, gerekli test ve eğitim faaliyetlerini tanımlayan kayıtların oluşturulması ve bilgi sistemleri süreklilik planının geliştirilmesi ve işletilmesinde görev alacak kişiler ile rol ve sorumlulukları belirlenerek ilgili eğitimleri almaları ve bu eğitimlere ilgili personel ve BGY Yöneticisinin katılımı sağlanır.

B. TEKNİK GÜVENLİK POLİTİKALARI:

B.1) Kullanıcı Parola Politikası:

(1)Tüm kullanıcılar etki alanına dâhil olan donanımlarında Kurumumuz tarafından sağlanan hizmetlerden faydalanmak için sisteme giriş yapmalıdır. Tüm kullanıcıların kullanıcı-kimliği (USER-ID varsa e-anahtarı) ve sadece kullanıcının bildiği şifre ile kimlik doğrulamasının yapılması zorunludur.
(2) Her kullanıcı, kendine ait hesabı kullanarak işlemlerini yürütür. Kullanıcılar kendi hesaplarının güvenliğini, şifrelerini saklayarak, başkalarının kendi hesabını kullanmasına izin vermeyerek ve gerektiğinde oturum kilitleme gibi özellikleri kullanarak korumakla yükümlüdürler.
(3) Kullanıcıya verilen ilk şifre veya şifresini unuttuğu zaman verilen şifreler “geçici şifre” olarak düşünülmeli ve ilk oturum açılışında hemen değiştirilmelidir.
(4) Kullanıcıların şifreleri en az 8 karakterli, büyük harf, küçük harf, noktalama işareti ve rakam özelliklerinden en az üçünü içeren karmaşık şifrelerden belirlenmeli, maskelenmiş olmalı ve geçerlilik süresi 60 gün süre olmalıdır.
(5) Kurum personeli şahsi şifrelerini ve var ise e-anahtarını özel kontrol altında tutmalı, şifrelerini sistem yöneticisi de dâhil olmak üzere hiç kimseyle paylaşmamalıdır.
(6) Kullanıcılar, Kurum servisleri için kullandıkları şifreleri, Internet üzerinde başka amaçlar için (örneğin tartışma gruplarına üyelik, gmail gibi bedava e-posta hesapları vb) kullanmamalıdır.
(7)Şifreler, dosya, otomatik komut dosyası (log-in script), yazılım makrosu, erişim kontrolü olmayan bilgisayarlar ve yetkisiz personelin fark edebileceği yerlere (kâğıt üzerine yazarak bilgisayarın yanına bırakmak gibi) yazılmamalıdır.
(8) Kullanıcılar, bilgisayarlarını kilitlemeden kullanılır durumda bırakmamalıdırlar.
(9) Kullanıcıların başarısız kimlik doğrulama girişimlerinde bulunarak, belirli sayıda art arda başarısız kimlik doğrulama girişimi durumunda ilgili kullanıcı erişiminin engellenmesi ve girişimde bulunan kişiye sistem veya kullanıcıya ilişkin bilgi verilmemesi sağlanır.
(10)Kullanıcılar, kullanmaya kısa süreli ara verdikleri bilgisayarları parola korumalı ekran koruyucu gibi özellikler kullanarak güvenlik altına almakla yükümlüdürler. Sistem tarafında da kullanılmayan bilgisayarların 5 dk. sürede ekran kilitlenmesine otomatik geçişi sağlanmaktadır.
(11) Etki alanı denetçileri kullanıcıların belirtilen sürelerde şifrelerini değiştirmeye zorlanmalıdır.

B.2) Taşınabilir Cihazlar Kullanım Politikası:

(1)Taşınabilir cihazlar; kurum bilgisi taşıyan her türlü dizüstü bilgisayar, akıllı telefon, CD, USB disk, teyp, taşınabilir sabit disk, yazılı raporlar gibi veri saklayabilecek ortamları tanımlamaktadır.
(2)Taşınabilir cihazlardaki bilgilerin üçüncü taraflarla paylaşımında da gerektiği kadar bilgi verme prensibi göz önünde bulundurulmalıdır.
(3)Kurum dışına çıkarılabilen varlıklar kurum dışında çalışırken gizlilik prensipleri ve varlık sınıflandırmaları göz önünde bulundurulmalı ve bilgi varlıklarının dışarı çıkarılabilmesine varlık sınıflandırması sonucuna uygun olduğu takdirde izin verilmelidir.
(4)Dizüstü bilgisayar, belge, CD gibi taşınabilir kurum varlıklarının korunması için gerekli önlemlerin alınmasından envanter sisteminde varlık sahibi olarak kaydedilmiş kişi sorumludur.
(5)Dizüstü bilgisayarlarda virüs taramaları en az iki haftada bir kez yapılmalı, virüs güncellemeleri çevrimdışı olarak kurum bilgi sistemleri üzerinden gerçekleştirilmelidir.
(6)Personelin kullanımı için tahsis edilmiş olan dizüstü bilgisayar, mobil cihazlar, tablet vb. sadece yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır.
(7)Kurum bilgi sistemleri kapsamında üretilen her türlü bilginin USB Bellek, CD vb ortamlarda saklanması kesinlikle yasaktır. Böyle bir durum gerekliliğinde BGY Yöneticisinin onayının alınması zorunludur.
(8) Mobil uygulamaların, güvenlik güncellemelerini kullanıcılara otomatik olarak bildirmesi sağlanır. Kritik güvenlik güncellemelerinin yapılması için kullanıcılar zorlanır ve uygulamanın eski sürümleri devre dışı bırakılır.
(9) Mobil uygulamaların çalıştıkları cihaza özgü güvenlik gereksinimlerine uygunluğu sağlanır. Bu uygulamalar yalnızca gerekli cihaz izinlerini talep eder ve kullanıcıların onayı alınarak en az izinle çalıştırılır.
(10) Mobil uygulamalarda aynı kullanıcı hesabıyla birden fazla cihazda eş zamanlı oturum açılması engellenir.
(11) Müşteri kullanımına sunulan mobil uygulamaların cihaz tanıma özelliğine sahip olması sağlanır.
(12) Mobil uygulamaların çalıştığı cihazlardaki hassas verilerin güvenliğini sağlamak ve bu cihazların işletim sistemi yazılımının kırılması veya değiştirilmesi gibi hallerden kaynaklanacak risklerin azaltılması amacıyla günün teknolojisine uygun kontroller tesis edilir.
(13)Mobil uygulama kontrolünde olmayıp cihaz üreticisi kontrolünde olan parola, PIN ya da biyometrik veriler, müşterinin bildiği ya da biyometrik karakteristiği olan unsurlar olarak kabul edilmez.

B.3) Sosyal Medya Kullanım Politikası:

(1) Kurum çalışanları kendisinin ve Kurum mobil cihazları ve bilgisayarları ile kuruma ait herhangi bir doküman, belge, fotoğraf ve benzeri bir paylaşım yapılması yasaktır.
(2)Kurumun bilgisayar ve iletişim sistemleri, personelin söz özgürlüğü hakkı için kullanılmamalıdır. Aksi davranışlar resmi soruşturmaya yol açar.

B.4) İnternet ve E-Posta Kullanım Politikaları:

(1) Kurum internet sistemi yalnızca iş faaliyetlerini destekleyecek şekilde kullanılmalıdır. Internet kullanımında; Kişisel kullanımda, görev amaçlı kullanılabilecek kaynaklar az miktarda kullanılıyorsa, Çalışanların verimliliğini engellemiyorsa, Herhangi bir iş faaliyetini aksatmıyorsa, Kullanıcıların bazı kişisel işlerini daha hızlı yerine getirmesini sağlıyorsa, kullanıma izin verilebilir.
(2) Kullanıcıların Internet kullanım yoğunluğu diğer kullanıcıların Internet'e ulaşımlarını engelleyecek şekilde olmamalıdır. Güvenlik yöneticileri, sistem yöneticileri ve bilgisayar operatörleri gibi sistem bakım-idame işlerini yürüten personele ayrıcalıklar tanınabilir.
(3) Internet kullanımı, içerik kontrolcüleri ve virüs tespit sistemleri kullanılarak sınırlandırılmaktadır. Kullanıcılar, bu kontrollerin yapıldığını bilerek Internet'i kullanmalı, güvenlik amacıyla konulan önlemleri devre dışı bırakmaya çalışmamalıdır.
(4) Çalışanlar kendi kullanımlarına kayıtlı olanlardan başka e-posta / iletişim ağı / uygulama hesaplarını kullanamazlar.
(5) Elektronik mesajlarda veya göndermelerde ihtiva edilen kullanıcı adı, elektronik posta adresi, organizasyonel bağlantı ve ilgili bilgi, mesajı yazan kişiyi yansıtmalıdır.
(6) Kuruma ait elektronik haberleşmenin, kişiye özel olacağını garanti edemez. Personel elektronik haberleşmenin, teknolojiye bağlı olarak, başkaları tarafından aktarılabileceğinin, engellenebileceğinin, yazıya dökülebileceğinin ve depolanabileceğinin farkında olmalıdır.
(7) Elektronik haberleşmenin içeriğinin düzenli olarak izlenmesi şirket politikasının bir parçası değildir. Ancak şüphelenilen mesajların incelenme hakkına ve yetkisine sahiptir. Bununla birlikte Internet üzerinden yapılan elektronik haberleşmenin içeriği izlenebilir ve elektronik haberleşme sistemlerinin kullanımı işlevsel, bakım, teftiş, güvenlik, araştırma faaliyetlerini desteklemek için izlenebilir.
(8) Genellikle kabul edilen iş uygulamalarına uyumlu olarak, kurumun elektronik haberleşme ile ilgili istatistiksel bilgiler toplama hakkına sahiptir. Bu bilgileri kullanarak teknik bu sistemlerin devam eden güvenirliliğini ve

kullanılabilirliğini emniyet altına almak için izlenebilmektedir. Bu yüzden personel, şirket tarafından konulan kısıtlamalara bağlı olarak Internet'ten kullanılan kaynaklar açısından adını gizleme şansına sahip değildir.
(9) Personel, üçüncü şahıslarla ilgili elektronik mesajlarda küfürlü, ayıp veya küçültücü ifadeler kullanmamalıdır. Bu tip ifadeler şaka yaparken bile kişisel iftira gibi yasal sorunlar yaratabilir.
(10) Kurum e-posta sunucusuna gelen mesajlar spam tarayıcısından geçirildikten sonra kullanıcılara ulaştırılmaktadır, ancak yine de kullanıcılar, e-posta vasıtasıyla bulaşabilecek virüs gibi zararlı içerikten korunmak amacıyla, tanımadığı kişilerden gelen ve şüpheli eklentiler içerdiği görülen mesajları gerekmediği sürece açmamalıdır.
(11) Kullanıcılar her türlü bilgi güvenlik alarmlarını, ikazlarını, şüpheli ihlalleri ve bunun gibi olayları derhal Bilgi Güvenliği İhlal Olayı Bildirim ve Yönetim Talimatına uygun olarak rapor etmekle sorumludurlar. Kullanıcıların, diğer kullanıcılara ister kurum içinde olsun ister kurum dışında olsun, şirket e-mail adreslerini kullanarak kurum haberleşme bilgileri harici gönderimler için Kurum, sistemlerinden faydalanmaları yasaklanmıştır.
(12) Elektronik posta sistemleri önemli bilgilerin arşiv depolamasına uygun değildir. Depolanmış önemli elektronik posta mesajları sistem yöneticileri tarafından periyodik olarak silinebilir, kullanıcılar tarafından kaza ile silinebilir ve sistem problemleri meydana geldiğinde kaybolabilir.
(13) Uzun süreli saklanması gerekli olmayan mesajlar periyodik olarak kullanıcılar tarafından kişisel elektronik mesaj saklama alanlarından silinmelidir. Belirli bir süreçten sonra çok kullanıcılı sistemlerde saklanan elektronik mesajlar otomatik olarak sistem yönetim personeli tarafından silinecektir. Bu, az olan saklama alanını çoğaltmakla kalmayıp, kayıt yönetimini ve ilgili faaliyetleri de kolaylaştıracaktır.
(14) Kurum bilgisayarlarına veya ağlarına gönderilen her türlü bilgiyi sansür etme yetkisini saklı tutar. Kurum suç veya kanunsuz olması muhtemel olarak görülen her türlü malzemeyi kendi bilgi sistemlerinden çıkarma hakkını ve bununla ilgili resmi işlem başlatma hakkını saklı tutar.

C. BİLGİ SİSTEMLERİ EDİNİMİ, GELİŞTİRİLMESİ VE BAKIMI:

(1) Kurum içinde geliştirilecek, değiştirilecek veya dışarıdan hizmet alımıyla temin edilecek bilgi sistemlerinin fonksiyonel gereksinimleri ile tasarım, geliştirme ve test aşamalarının her biri için teknik ve güvenlik gereksinimleri yazılı hale getirilir.
(2) Bilgi sistemlerinde yapılacak önemli güncellemelerin veya değişikliklerin iş süreçlerini aksatmaması ve bilgi güvenliği riski oluşturmaması için güncelleme veya değişikliklere ilişkin planlama, test ve uygulama adımları detaylı olarak ele alınır.
(3) Yazılım geliştirme süreçlerinde görev alan personelin güvenli yazılım geliştirme konusunda eğitim alması sağlanır.
(4) Geliştirme, test ve gerçek ortamlar yetkisiz erişim ve değişim riskine karşı birbirinden ayrılır. Test ortamındaki veriler, müşteri bilgilerini içermeyecek ve gerçek ortamdaki işlemlerle uyumlu olacak şekilde belirlenir.
(5) Bilgi sistemleri gerçek ortamda kullanıma alınmadan önce kabul kriterleri belirlenir, hazırlanacak bir plana göre fonksiyonel, teknik ve güvenlik gereksinimleri testlerine tabi tutulur, gerçek ortama alınması onay sürecine bağlanır. Kritik uygulamalar gerçek ortama alınmadan önce güvenlik testlerinden geçirilir, tespit edilen bulgular giderilir.
(6) Uygulama geliştiricilerin zorunlu olmadıkça gerçek ortama erişimleri engellenir. Gerekmesi durumunda, bilgi güvenliği sorumlusunun onayı alınarak ve yapılan tüm işlemlerin denetim izleri tutularak kısıtlı süreyle erişim sağlanır.

D. İŞ SÜREKLİLİĞİ YÖNETİMİ:

(1) Bilgi sistemleri süreklilik planının geliştirilmesi ve işletilmesinde görev alacak kişiler ile rol ve sorumlulukları belirlenerek ilgili eğitimleri almaları sağlanır. Planın devreye alınması kararını verecek kişi ve durumlar yazılı hale getirilir. Bilgi sistemleri süreklilik planı üst yönetim tarafından onaylanır. Planın sadece ilgili kişiler tarafından erişilebilir olması ve güncel fiziksel kopyalarının gereken yerlerde bulundurulması sağlanır.
(2) Planda yer alan süreçlerin her biri için kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı değerleri belirlenir. Bu çerçevede hizmetlerin tekrar kullanıma açılmasını sağlayacak alternatifli kurtarma süreç ve prosedürleri tesis edilir ve gerekli önlemler alınır.
(3) Bilgi sistemlerinden kaynaklanabilecek kesintilere, işlem performansını düşürecek veya iş sürekliliğini aksatacak durumlara karşı gerekli önlemler alınır.
(4) Bilgi sistemlerinin sürekliliğini sağlamak amacıyla, risk değerlendirmesi, risk azaltma ve risk izleme faaliyetleri gerçekleştirilir.
(5) Plan, iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra veya yılda en az bir kez gözden geçirilerek güncellenir. Planın etkinliğini ve güncelliğini temin etmek üzere testler yapılır, testlere varsa dışarıdan hizmet alınan kuruluşlar da dâhil edilir ve test sonuçları üst yönetime raporlanır. Testler her yıl tekrarlanır.
(6) Bilgi sistemleri, iş sürekliliği planındaki önceliklere uygun olarak yedeklenir ve yedekten geri dönülmesi için gerekli süreçler bilgi sistemleri sürekliliği planına ve testine dâhil edilir. Bu kapsamda yedekleme çizelgesi

hazırlanır, üst yönetime onaylatılır ve güncelliği sağlanır. Yedeklerin en az bir kopyası farklı coğrafi bir konumda saklanır. Yedeklerin güvenliğine ilişkin gerekli önlemler alınır.
(7) Yılda en az bir defa asgari olarak kritik sistemlerin yedekten geri dönme testi gerçekleştirilir ve teste katılanların bilgisi, tarih, testin detayları ve sonuçları kayıt altına alınır. Alınan yedeklerin yasal saklama süresi boyunca geri döndürülebilir olması sağlanır.
(8) Kurum faaliyetlerini iş sürekliliği planında belirlediği kabul edilebilir kesinti süreleri ve azami veri kaybı değerleri dahilinde sürdürmesini sağlayacak şekilde bilgi sistemlerinde gerekli altyapıyı kurar.
(9) Şirket bilgi güvenliği politikasının, bilgi sistemleri süreklilik planının, bilgi varlıkları envanteri ile iş sürekliliği ve güvenliği açısından önem arz eden diğer dokümanların güncel sürümlerini ve bilgi sistemleri yönetimine ilişkin parolalarını güvenli ortamlarda saklar.

E. UYUM SÜRECİ:

(1) Kurumca uygulanan bilgi güvenliği politikası, yürürlükteki tüm kanunlarla uyumlu olmak zorundadır.
(2) Kurumda kullanılmakta olan tüm yazılımların lisans sözleşmeleri olmak zorundadır. Lisanssız ürünlerin kurum varlıklarında kullanılması yasaktır.
(3) Herhangi bir bilişim suçu işlediği saptanan personel, yasalara uygun olarak cezai işlem görür.
(4) Bilişim suçları kapsamı yasalar takip edilmeli, yasal düzenlemelerde bilgi güvenliği politikasını etkileyen bir değişiklik belirtildiğinde, politika güncellenmelidir.
(5) Bilgi güvenliği olayı için kanıt oluşturabilecek herhangi bir veri, yetkililer gelene kadar değişime uğramayacak ve kanıt özelliğini kaybetmeyecek şekilde saklanmalıdır.

F. YÜRÜRLÜK VE YÖNETİMİN ONAYI:

İşbu Bilgi Güvenliği Politikası 30.06.2025 tarihli Yönetim Kurulu kararı ile onaylanır ve Tebliğ'deki uyum süresi gözetilerek yürürlüğe girer.

Bilgi Güvenliği Politikasında herhangi bir değişiklik gerektiğinde, değişiklik yapılan hususlar Yönetim Kurulu onayından geçtikten sonra geçerlilik kazanır. Onaylanan Bilgi Güvenliği Politikası tüm çalışanlarına ve konu ile ilgili olanlara duyurulur.

G. ÇALIŞANIN/ İLGİLİNİN ONAYI:

Üstte yazan maddeleri okudum, anladım ve kabul ediyorum.
(Lütfen bu ifadeyi el yazısıyla yazıp imzalayınız.)