KISALTMALAR

ASB	Bilgi İşlem Daire Başkanlığı Ağ ve Sistem Birimi
BGYS	Bilgi Güvenliği Yönetim Sistemi
BS	Bilgi Sistemleri
EBYS	Elektronik Bilgi Yönetim Sistemi
FKM	Felaket Kurtarma Merkezi
İEA	İş Etki Analizi
KBTS	Kurumsal Bilgisayar Tanımlama Sistemi
KEP	Kamu Elektronik Posta Sistemi
NTP	Network Time Protocol
SOME	Siber Olaylara Müdahale Ekibi
ÜBYS	Üniversite Bilgi Yönetim Sistemi
VPN	Sanal Özel Ağ
YGG	Yönetimin Gözden Geçirmesi Toplantısı

TANIMLAR

Gizlilik Sözleşmesi	Bilginin gizli olduğunun bildirimini vermek için kullanılan ifşa etmeme anlaşmalarıdır.
İş Etki Analizi	İşin kesintiye uğraması üzerinde etkisi olabilen faaliyetlerin ve etkisinin analiz edilmesi sürecidir.
İş Sürekliliği	Kesinti olayının yaşanmasından sonra ürün ve hizmetlerin kabul edilebilir seviyelerde sunumuna devam etme konusunda Kurum'un sahip olduğu yetenektir.
İş Sürekliliği Planı	Kesintinin ardından karşılık verme, kurtarma işlerini yapma, sistemi yeniden başlatma ve önceden tanımlanan iş seviyesini yeniden kazanma konusunda Kurum'a yol gösteren yazılı süreçlerdir.
Kritik Faaliyet	Yaşanabilecek olası bir kesintinin etkisinin Kurum için çok kısa zamanda çok yüksek seviyelere çıkabildiği, Kurum itibarına, yasal, mali ve müşteri ilişkilerine etkisi olan faaliyetlerdir. "Kritik" ve "önemli" ifadeleri birbiri ile karıştırılmamalıdır. Kurum için "önemli" olan bir faaliyet, geliştirilen ürün ve hizmetler için "kritik" olmayabilir.
Kurum	Kastamonu Üniversitesi
Olay	İş sürekliliğini kesintiye uğratan risk seviyesi düşük her türlü durumdur.

Satın Alma Sorumlusu	Belirli bir satın alma talebinin gerçekleştirilebilmesi için Satın Alma Birimi İç/Dış/İhaleli Satın Alma Koordinatörleri tarafından talep içeriğine göre seçilen ve satın alma talebi yönlendirilen Satın Alma Birimi çalışanıdır.
Sızma Testi	Penetrasyon Testi (Pentest)
Tatbikat	Kurum performansının değerlendirilmesi, uygulanması ve iyileştirilmesi için yıllık olarak gerçekleştirilen eğitim/öğretim faaliyetleridir.
Yönetim Birimleri	Kurum'a bağlı tüm fakülte, yüksekokul, enstitü, koordinatörlükler ve idari birimler.

1. AMAÇ:

Bilgi Güvenliği Uygulama Politikalarının amacı; Kastamonu Üniversitesi çalışanlarının, sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından yapılması, uyulması gereken iş kurallarını hedeflemek ve bu hedefler kapsamında iş sürekliliğini sağlamaktır.

Kurumun amacı herhangi kimse üzerinde kısıtlayıcı politikalar üretmek değil, aksine açıklık, güven ve bütünlüğe yönelik kültürü yerleştirmektir. Kurum bilerek / bilmeyerek yapılan, yasadışı veya zararlı eylemlere karşı çalışanın ve kurumun haklarını koruma altına almaktadır. Bilgi teknolojileri ile alakalı sistemler kurumun sahip olduğu değerlerdir. Güçlü bir bilgi güvenliği bütün çalışanların dâhil olduğu takım çalışmasıyla gerçekleştirilir. Bilgi güvenliğinin sağlanabilmesi için bütün personelin bilgi güvenliği politikalarını iyi bilmesi ve uygulamanın sorumluluğunu taşıyabilmesi gerekmektedir.

2. KAPSAM:

Bilgi ve İletişim Güvenliği Genelgesi dâhilinde yapılan işlemler.

3. YAPTIRIM:

Bu politikalara uygun olarak hareket etmeyen çalışanlar ile öğrenciler hakkında ilgili kanun, yönetmelik ve diğer mevzuatların hükümleri uygulanacaktır. Tedarikçi ve ziyaretçiler için ise ilgili mevzuat hükümleri uygulanarak yasal süreç başlatılacaktır.

4. SORUMLULAR:

Bilgi Güvenliği Uygulama Politikalarının, gözden geçirilmesi ve güncellenmesinden Rektörlük Makamı Onayı ile oluşturulan Bilgi Güvenliği Ekibi sorumludur. Üniversite Senatosu tarafından Bilgi Güvenliği Politikası onaylanır ve Bilgi İşlem Daire Başkanlığı tarafından duyurulur. Bu politikalardan bütün çalışanlar, öğrenciler, tedarikçiler ve ziyaretçiler sorumludur.

5. UYGULAMA:

5.1 POLİTİKA LİSTESİ

- P01 İnternet Erişim Politikası
- P02 E-Posta Politikası
- P03 Anti-Virüs Politikası
- P04 Şifre Politikası
- P05 Fiziksel Güvenlik Politikası
- P06 Sunucu Güvenlik Politikası
- P07 Ağ Yönetimi Politikası
- P08 Uzak Bağlantı Politikası
- P09 3. Taraf Güvenlik Politikası
- P10 Kabul Edilebilir Kullanım Politikası
- P11 Temiz Masa Temiz Ekran Politikası
- P12 Mobil Cihaz Politikası
- P13 Veri Tabanı Güvenlik Politikası
- P14 Yazılım Temini ve Geliştirme Politikası
- P15 Değişim Yönetimi Politikası
- P16 Olay Yönetim Politikası
- P17 Kripto Grafik Kontroller Politikası
- P18 Kamera Politikası
- P19 Yedekleme Politikası
- P20 Web Sayfası Tahsisi Politikası
- P21 Erişim Kontrol Politikası
- P22 İş Sürekliliği ve FKM Politikası
- P23 Log Yönetimi Politikası
- P24 Sanallaştırma Politikası
- P25 Sosyal Medya Politikası
- P26 Tedarikçi İlişkileri Bilgi Güvenliği Politikası
- P27 Uzaktan Çalışma Politikası
- P28 Veri Envanteri Politikası
- P29 Zafiyet ve Yama Yönetimi Politikası

5.2 BİLGİ GÜVENLİĞİ UYGULAMA POLİTİKALARI

P01 İNTERNET ERİŞİM POLİTİKASI

1. Amaç

Kurum içinde güvenli internet erişimi için sahip olması gereken standartların uygulanmasını amaçlamaktadır. İnternetin uygun olmayan kullanımı; kurumun yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenmeyen sonuçlara neden olabilir. Bu tür olumsuzlukların gerçekleşmemesi için etik ve yasalar çerçevesinde internet kullanım kurallarını belirlemektir.

2. Kapsam

Bu politika kurum internetini kullanan çalışanları, öğrencileri, tedarikçileri ve ziyaretçileri kapsamaktadır.

3. Politika

- Kurum ağlarına bağlı bütün bilgisayarlar içerik denetimi yapan bir uygulama üzerinden internete çıkacaktır. Üniversite bünyesinde Eğitim, Öğretim, idari, akademik amaçlara ve yasalara uygun olmayan tüm siteler yasaklıdır. Ancak yetkilendirilmiş sistem yöneticileri ve kişiler internete çıkarken bütün servisleri kullanma hakkına sahiptir.
- 5651 sayılı kanun (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) gereği kurum internet erişim kayıtları en az 24 ay arşivlenmektedir.
- Bilgisayarlar üzerinden yasalara aykırı internet sitelerine girmek ve dosya (f ilm, müzik, program vb.) indirmek yasaktır.
- Vpn ve proxy dışındaki diğer tüm Tunnel platformları ve dns değişiklikleri yapılarak internete bağlanılması yasaktır.
- Başkalarının fikri haklarını ihlal edici mahiyette (copyright) materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.

- Sistem ve ağ güvenliğinin ihlal edilmesi yasak olup, cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum, bu tür ihlallerin söz konusu olduğu durumları inceler ve bir suç oluştuğundan şüphe duyulursa ilgili kanun, yönetmelik ve diğer mevzuatların hükümleri uygulanabilir veya yasa uygulayıcısı ile iş birliği yapılabilir.

- İnternet üzerinden uygunsuz, müstehcen, rahatsız edici materyaller ile kuruma ve kurumun çalışanlarına, bunların aile fertlerine veya Türkiye Cumhuriyeti Devletine, ulusuna, yasama, yürütme ve yargı organlarına, askeri ve emniyet teşkilatına, vatandaşların a yönelik iftira, karalama mahiyetinde mesajlar yayınlamak ve paylaşmak yasaktır.

- Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek, zarar verebilecek, etik olmayan veya yasalara uygun olmayan çevrimiçi olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınları kullanması yasaktır.

- Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, Üniversitenin kurumsal imajını zedeleyici ve yasalarla da yasaklı bulunan site ve forum vb. gibi sayfalara kurumsal e-posta adresleri ile üye olması yasaktır.

- Kullanıcıların kurum hesaplarına ait kullanıcı adı ve şifreleri internet üzerinden paylaşması yasaktır.

- Kullanıcıların kurum internet ağı üzerinden yaptığı kişisel işlemlerde (banka, alışveriş, e- posta vb.) oluşacak olumsuzluklardan kurum sorumlu değildir, bu tür sebepler ile kurum veya kişisel hesabının bir başkasının eline geçmesine sebep olunması ve bu durumda gerçekleştirilebilecek muhtemel suçlardan kişi mesuldür.

- İnternette gezinirken reklam veya bilgi çalmak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.

- **P02 E-POSTA POLİTİKASI**

1. Amaç

Kurumsal e-postaların standartlara uygun, kesintisiz kullanım ve güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bu politika kurum e-postasını kullanan çalışanları ve öğrencileri kapsamaktadır.

3. Politika

- Kullanıcıların kurum e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar Kastamonu Üniversitesi'nin bilgi varlığıdır. Bu nedenle Bilgi İşlem Daire Başkanlığı kurumsal e-postaları adli mercilerin istemesi ya da mahkeme kararı olması durumlarında haber vermeksizin denetleyebilir ve yasa uygulayıcıları ile paylaşabilir.

- Kastamonu Üniversitesi, kurum ile ilişiği kesilmesi durumunda kullanıcıların kurumsal e-postalarına erişimini gerek gördüğünde engeller ve kullanıcılar ile e-posta yedeklerini paylaşma zorunluluğu yoktur.

- İlişiği kesilen kullanıcıların e-posta hesapları devre dışı bırakılır, e-postalarına erişimleri engellenir. Mahkeme kararı ile ilgili hesaplara erişim talebi yapılması durumunda, e-postalar ilgili kişi/kurum ile paylaşılabilir. Kullanıcının Kurumdan ayrılmasından 2 (iki) yıl sonra hesap silinir.

- Kastamonu Üniversitesi ile ilgili Gizli/Kritik verileri içeren bilgiler elektronik posta, internet dosya paylaşım siteleri, paylaşım yazılımları ile tutulamaz ve gönderilemez.

- Kastamonu Üniversitesi'nin e-posta gruplarına, kişisel kullanım amaçlı e-posta gönderilmesi yasaktır. Bilimsel, akademik ve idari iş süreçlerine uygun toplu duyurular ise Kastamonu Üniversitesi Basın Yayın Müşavirliği aracılığı ile yapılabilecektir.

- Kurumsal e-posta; yasadışı, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik, spam, zincir e-posta ve bu e-postalara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postaların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir e-posta alındığında hemen Bilgi İşlem Daire Başkanlığı'na veya Bilgi Güvenliği Ekibine haber verilmesi ve yetkili kişiler müdahale edene kadar e-postanın silinmemesi, cevaplanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

- E-posta gönderen çalışan, e-posta içeriğini dikkate alarak, sadece ilgili kişilere göndermelidir. E-posta gönderilmeden önce "kime" ve "bilgi" bölümlerine eklenen kişi listesi kontrol edilmelidir.

- Kullanıcılar, e-posta ile istenen mail içeriğinde kullanıcı adı ve şifre paylaşmamalıdır. Kullanıcı adı ve şifre talep edilen e-postalar alındığında hemen Bilgi İşlem Daire Başkanlığı'na veya Bilgi Güvenliği Yönetim Sistemi Ekibine haber verilmeli ve yetkili kişiler müdahale edene kadar e-posta silinmemeli, cevaplanmamalı, iletilmemeli ve içeriğine tıklanmamalıdır.

- Kullanıcıların; kurumsal e-posta ile uygun olmayan içeriklere sahip e-posta (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyeti ihlal eden ve hakaret içeren vb.) göndermeleri yasaktır.

- Kurum akademik, idari ve sözleşmeliler ile işçi statüsündeki personelin e-posta hesabı açılması için https://bidb.kastamonu.edu.tr adresindeki dokümanlar kısmında "kişisel e-posta istek formunu" doldurması ve imzalayarak Bilgi İşlem Daire Başkanlığı Sekreterliğine ulaştırması gerekmektedir.

- Üniversitede hizmet alımı ile çalışan personele e-posta hesabı açılması için personelin https://bidb.kastamonu.edu.tr adresindeki dokümanlar kısmında kişisel e-posta istek formunu doldurması ve bağlı olduğu birimin amirine ıslak imzalatarak Bilgi İşlem Daire Başkanlığı Sekreterliğine ulaştırması gerekmektedir.

- Üniversitede öğrenim gören yüksek lisans ve doktora öğrencilerinin https://bidb.kastamonu.edu.tr adresindeki dokümanlar kısmında bulunan öğrencilere ait olan e-posta istek formunu doldurarak Bilgi İşlem Daire Başkanlığı Sekreterliğine teslim etmesi gerekmektedir. Üniversitemize yeni kayıt yaptıran öğrencilerin ise Öğrenci Bilgi Sistemi üzerinden öğrenci numaraları temin edilerek öğrenci_numarası@ogr.kastamonu.edu.tr şeklinde otomatik olarak açılmaktadır.

- Üniversitede faaliyet gösteren fakülte, enstitü, yüksekokul, meslek yüksekokulu; bölüm, başkanlık, müdürlük, koordinatörlük, müşavirlik, anabilim dalı, sempozyum vs. gibi bütün kurumsal noktalara e-posta adresi tanımlanabilmesi için https://bidb.kastamonu.edu.tr internet adresindeki dokümanlar kısmından kurumsal e-posta istek formunun doldurularak e-posta, birim sorumlusunun ve birim amirinin imzasıyla birlikte üst yazı ile Bilgi İşlem Daire Başkanlığına gönderilmesi gerekmektedir.

- Kurumsal e-postalar için görevlendirmesi yapılan personelin birimi ile ilgisi kalmadığı durumda yeni görevlendirilen personelin yazısı birim amiri ve görevli personel tarafından onaylanarak Bilgi İşlem Daire Başkanlığına gönderilmelidir.

- Kullanıcı, gizli mail içeriğini ilgisi bulunmayan kişilere göstermeyeceğini, hizmet hakkının sadece kendisine ait olduğunu, bu hakkın kullanımına ilişkin özel ve gizli şifresini ve kullanıcı adını ve/veya kodunu başkasına kullandırmayacağını ve devretmeyeceğini, başkası tarafından öğrenilme şüphesi dahi olsa derhal değiştireceğini, aksi takdirde yapılan bütün işlemlerin sorumluluğunun kendine ait olacağını, kendisi kullanmadığı iddiası ile sorumluluktan kurtulamayacağını kabul eder.

- Kastamonu Üniversitesi personelinin, kurum kimliği altında sürdürülen bütün faaliyetler için kuruma ait elektronik posta adresine sahip olması ve ilgili yazışmalar için "@kastamonu.edu.tr" uzantılı e-posta hesabını kullanması gerekir.

- Kullanıcı, hesabında ve/veya sitesinde ticari reklamlara ve üyelik ile sağlanan yerli/yabancı destekleyici (sponsor) reklamlarına, bağlantılarına yer veremez. Ticari reklamlar ve haber duyuruları gibi istenmeyen mesajlar gönderemez.

- Kullanıcı şifresi sadece kullanıcı tarafından bilinir. Kullanıcı ilk kullanımdan itibaren dilediği zaman e-posta şifresini değiştirebilir. Şifrenin seçimi ve korunması tamamıyla kullanıcının sorumluluğundadır. Şifre değiştirme işlemi https://passwordreset.microsoftonline.com/passwordreset#!/ adresinden ya da Microsoft 365 hesabının içerisindeki şifre değiştirme ara yüzünden yapılabilmektedir. Kullanıcılar, şifrelerini unutmaları durumunda https://passwordreset.microsoftonline.com/passwordreset#!/ adresinden yeni şifre alabilirler. Kullanıcı hesabı;

  - T.C. yasalarının belirlediği yasadışı kullanımlarda,
  - Kastamonu Üniversitesi tarafından belirlenen kullanım politikalarına uyulmadığı durumlarda,
  - Kullanıcı hesapları için belirlenen sınırların aşıldığı durumlarda,
  - Kastamonu Üniversitesi bilişim kaynaklarının akademik amaçlı çalışmaları engelleyici biçimde akademik amaçlı olmayan, ticari ve yasadışı amaçlı kullanıldığı durumlarda,
  - Kişilere ait kullanıcı hesaplarının farklı kişiler tarafından kullanımının belirlendiği durumlarda,

- Sunucu sistemler üzerinde tanımlı diğer kullanıcıların şifrelerini bulmaya çalışmak, dosyalarına müdahale etmek, değiştirmek vb. girişimlerin tespit edildiği durumlarda,
- Sistem doğruluğunun, bütünlüğünün, güvenliğinin ve servis devamlılığının engellendiği durumlarda kullanıcıya haber verilmeksizin Bilgi İşlem Daire Başkanlığı tarafından ya da sistem tarafından otomatik olarak erişime kapatılabilir. Kullanıcı hesabının kalıcı olarak kapatılacağı durumlarda kullanıcılar önceden bilgilendirilir.

- E-posta hesap sahibi üniversite personelinin tayin, istifa, emekli olma, sözleşme bitimi, ölüm, kayıp, meslekten ihraç gibi durumlarında ve öğrencilerin üniversiteden mezun olma, kayıt sildirme, yatay geçiş, okuldan atılma, ölüm durumlarında konunun Bilgi İşlem Daire Başkanlığı'na bildirildiği gün e-posta ve diğer kurumsal hesapları durdurulacaktır.

P03 ANTİ-VİRÜS POLİTİKASI

1. Amaç

Bilgisayar ve sunucuların zararlı yazılımlardan korunması amaçlanmaktadır.

2. Kapsam

Bu politika bütün bilgisayarları ve sunucuları kapsamaktadır.

3. Politika

- Kurumun bütün bilgisayarları ve sunucuları Anti-virüs yazılımına sahip olacaktır.
- Hiç bir kullanıcı herhangi bir sebepten dolayı Anti-virüs programını sistemden kaldıramaz veya durduramaz.
- Anti-virüs yazılımı düzenli aralıklar ile otomatik veya manuel olarak güncellenecektir.
- Anti-virüs yazılımı anlık olarak bilgisayar ve sunucularda virüs taraması yapacaktır.
- Virüs bulaşan makineler tam olarak temizleninceye kadar ağa bağlanmayacaktır. Bilgisayarlarda virüs olduğu uyarısı alındığında veya şüpheli durumlarda hemen Bilgi İşlem Daire Başkanlığı'na veya Rektörlük Makamı onayı ile oluşturulmuş Bilgi Güvenliği Yönetim Sistemi Ekibine haber verilmeli ve yetkili kişiler müdahale edene kadar bilgisayarın kullanılmaması gerekmektedir.
- İnternet üzerinden bilinmeyen ve şüpheli kaynaklardan indirilen dosyaların içerisinde virüs olabilir, bu tür kaynaklardan dosya indirilmesi yasaktır.
- Bilgisayarlarda kullanılacak CD, DVD, USB gibi depolama aygıtlarını ve internet üzerinden indirilen dosyaları virüs taraması yapmadan kullanmak yasaktır.
- Bilgi İşlem Daire Başkanlığı'nın hazırlamış olduğu bilgisayarlar güncellemeleri yapılmış anti virüs yazılımı yüklenmiş şekilde kurum ağına dâhil edilir. Bilgi İşlem Daire Başkanlığı kontrolü dışında alım yapılan veya kurum dışından gelen bilgisayarlara cloud.kastamonu.edu.tr adresinden lisanslı anti virüs programının indirilerek kurulması ve güncel tutulması zorunludur.

P04 ŞİFRE POLİTİKASI

1. Amaç

Bilgi Güvenliğinin arttırılması için güçlü bir şifreleme oluşturulması ve şifrelerin güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bilgisayar, sunucu, ağ cihazları, uygulama ve epostaları kullanan bütün kullanıcı hesaplarını kapsamaktadır.

3. Politika

- Bilgisayar kullanıcı hesaplarının şifreleri en az 8 karakter ve karmaşık şekilde büyük harf, küçük harf, rakam ve özel karakter (\ * ? - = / _ + % & vb.) kullanılması zorunludur.

- Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kolay tahmin edilen (Aa123456, Ab123456, Qaz12345, Asd12345, memleket, çocuk, çalışanın kendi ismi, doğum tarihi, ardışık rakam ve harfler, İstanbul, Kastamonu vb.) şifreler kullanılması yasaktır.

- Kurum içerisinde kullanılan bilgisayar, uygulama ve eposta hesap şifrelerinin yılda bir değiştirilmesi gerekmektedir. Aksi halde oluşabilecek sorunlardan kullanıcı sorumludur.

- Kurum içerisinde kullanılan sunucu hesap şifrelerinin yılda en az 1 kez değiştirilmesi zorunludur ve değiştirilen sunucu ve uygulamaların yönetici şifreleri kapalı zarfa konularak mühürlü bir şekilde üst yönetime teslim edilir.

- Kurum içerisinde kullanılan sunucu, hesap, e-posta vb. sistemlerin şifreleri, şifre bilgisine sahip personelin yer değişikliği ya da Kurumdan ayrılmasıyla birlikte değiştirilmesi zorunludur.

- Bilgisayarlar ve sunucularda işlem yapılmadığı sürece otomatik olarak 5 dakika sonrasında şifreli ekran koruması devreye girecektir.

- Bilgi İşlem Daire Başkanlığı tarafından oluşturulan yeni şifrelerin ilk kullanımdan itibaren değiştirilmesi zorunludur.

- Üst üste 5 kez hatalı şifre girildiğinde kullanıcı hesabı kilitlenecektir, bu gibi durumlarda Bilgi İşlem Daire Başkanlığı ile iletişime geçilmesi gerekmektedir.

- Kurumsal hesaplara ait şifrelerin herhangi bir kimseyle (iş arkadaşları, aile bireyleri vb.) paylaşılması yasaktır. Kurumsal kullanıcı hesabı ile yapılan tüm işlemlerden çalışanın kendisi sorumludur.
- Kurum bünyesinde bulunan aktif ağ cihazları (anahtar, yönlendirici, kablosuz erişim noktası vb.) ve ağ güvenliği cihazları (güvenlik duvarı, saldırı engelleme/tespit sistemleri, içerik filtreleyiciler vb.) için aşağıda tanımlanan kurallar çerçevesinde parola politikası uygulanır;
- Bilgi İşlem Daire Başkanlığı yönetimindeki donanım ve yazılımlar, varsayılan (default) parola ile kullanılmaz.
- Sistemler devreye alınmadan önce teknik olarak mümkün ise varsayılan hesaplar ve kurulum hesaplarının parolaları değiştirilir.
- Parola uzunluğu en az 12 (on iki) karakterden oluşur ve şifrelenmiş şekilde saklanır.
- Parola büyük harf, küçük harf, rakam veya noktalama işareti özelliklerinden en az üçünü içerir.
- Sistemlerin yönetici hesabı parolaları Bilgi İşlem Daire Başkanlığı tarafından şifreli bir ortamda saklanır. Parolalar, rol ve yetkilere göre gruplandırılarak (Sistem Yöneticisi, Ağ Yöneticisi, Son Kullanıcı Destek Sorumlusu vb.), bağımsız dosyalarda tutulurlar.
- Fiziksel Kasaya şifre ile erişim sağlanır. Şifre Bilgi İşlem Daire Başkanında ve en az bir Bilgi İşlem Daire Başkanlığı Şube Müdüründe bulunur.

- Kurumsal hesaplara ait şifreleri kâğıt veya elektronik ortamlara (e-posta, word, excel, forum siteleri, mesajlaşma uygulamaları vb.) yazılması ve paylaşılması yasaktır.

- Sistem yöneticileri kendi kullanıcı adı ve şifreleri ile sunuculara bağlanmalıdır, yerel yönetici (local admin) hesaplarının kullanılması yasaktır.

- Kullanıcı hesaplarına ait şifreler Bilgi İşlem Daire Başkanlığı tarafından kayıt altında tutulmamaktadır. Kullanıcıların bilgisayarlarında oturum açma işlemleri, şifre değişiklikleri ve Bilgi İşlem Daire Başkanlığı tarafından yapılan şifre değişiklik kayıtları (değiştirme ve oturum açma zamanı, bilgisayar ip adresi ve adı) sistemler üzerinde 2(iki) yıl süreyle saklanmaktadır.

- Kurum içinde kullanılan diğer uygulamaların (Yönetim programları, Firewall, Mail Gateway, Ortam Denetleme vb.) şifreleri de Şifre Politikası'na uygun olarak tanımlanacaktır.

- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de Şifre Politikası'na uygun olarak hazırlanacaktır.

P05 FİZİKSEL GÜVENLİK POLİTİKASI

1. Amaç

Kurumun bilgi varlıkları, ekipmanları ve alt yapı cihazlarının fiziksel güvenliği ve yetkisiz erişimlerinin önlenmesi amaçlanmaktadır.

2. Kapsam

Kurumun bilgi varlıkları, ekipmanları ve alt yapı cihazlarını kullananları kapsamaktadır.

3. Politika

- Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanacak ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilecektir.

- Kastamonu Üniversitesi'ne girişler ve koridorlar güvenlik açısından kamera ile kayıt altına alınarak izlenmektedir. Kamera kayıtları en az 20 gün saklanmaktadır.

- Açık ofislerde ve odalarda bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulacaktır.

- Kurumun bilgi varlıkları, bilgisayar ve çevre birimleri (harici diskler, yazıcı, monitör, projeksiyon vb.), alt yapı cihazlarını hasar / hırsızlık gibi oluşabilecek risklere karşı önlem almak ve güvenliği açısından uyarı yazıları yazmak kişi ve birimin kendi sorumluluğundadır.

- Kritik bilgi varlıkları ve altyapı cihazları kilitli odalarda ve kabinetlerde muhafaza edilecektir.

- Erişim yetkisi verilerek girilen alanların erişim yetkileri düzenli aralıklar ile kontrol edilecektir.

- Anahtar konumundaki tesislere herkesin erişimini engellemek için fiziki ve/veya elektronik tedbirlerin alınması sağlanır (Bilgi İşlem Daire Başkanlığı ofisleri, sistem odası, güvenlik odaları, gibi önem arz eden ofisler binaların merkezi ve en güvenli bölgelerinde yer almalıdır.)
- Bina ve tesislerin dış alanında çalışma faaliyetlerini belirten herhangi bir ipucu verecek işaret olmamalıdır.
- Bu bölgelerin girişlerinde "Girilmez" işareti bulundurulur.
- Kurum çalışanına bilmesi gereken prensibi esasına göre bilgilendirme yapılır.
- Kurum içerisinde tüm koridorlar, geçiş ve giriş-çıkış noktalarında, seçilmiş odalarda Güvenlik bünyesinde oluşturulan kamera sistemi ile gerçekleştirilir ve arşivlenir.

P06 SUNUCU GÜVENLİK POLİTİKASI

1. Amaç

Kurumun sahip olduğu sunucuların temel güvenlik kurallarını oluşturmayı amaçlamaktadır.

2. Kapsam

Bu politika kurumun sahip olduğu bütün sunucuları kapsamaktadır.

3. Politika

- Kurum bünyesindeki bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.
- Bütün sunuculara Bilgi İşlem Daire Başkanlığı'nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
- Kullanılmayan sunucular güvenlik, performans ve elektrik tasarrufu açısından kapalı tutulacaktır.
- Sunucuların, işletim sistemi, uygulamalar, veri tabanları ve ağ ekipmanlarının erişim logları ilgili cihazlarda en az 2(iki) sene saklanacaktır.
- Sunucuların kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak kontrol edilecektir.
- Sunucuların yönetimi için her kullanıcı kendi hesabı ile bağlantı yapacaktır. Sunuculara dışarıdan yapılan bağlantılar Uzak Bağlantı Politikası'nın belirlediği kurallara göre gerçekleştirilecektir.
- Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.
- Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenecektir.
- Sistem odası sıcaklık derecesi tavsiye edilen (22-24 ^{0}C) seviyede tutulacak şekilde soğutulacaktır.
- Sistem odalarına giriş ve çıkışlar erişim kontrolü olacak ve kayıt altına alınacaktır.
- Sistem odalarındaki ekipmanların bakımları düzenli olarak yapılacak ve bakım kayıtları tutulacaktır.

- Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunacaktır, yangın ve benzer felaketlere karşı koruma altına alınacaktır.
- Sunucularda anti-virüs programı yüklü olacak ve anlık olarak tarama yapacaktır.

P07 AĞ YÖNETİMİ POLİTİKASI

1. Amaç

Kurumun bilgi teknolojileri ağında yer alan bilgilerin, ağ alt yapısının ve ekipmanlarının güvenliğini ve sürekliliğini sağlamayı amaçlamaktadır.

2. Kapsam

Kurum bünyesindeki ağ altyapısı, donanım ve kullanıcıları kapsamaktadır.

3. Politika

- Üniversitenin ağ alt yapısındaki, donanımı ve yazılımı zarara uğratan, tahrip edici, zedeleyici ve sağlıklı çalışmasını engelleyici hiçbir girişimde bulunulmaması; kaynakların verimli kullanılması en temel ilkedir.

- Üniversitenin ağ hizmetleri Türkiye Cumhuriyeti yasalarına ve Üniversite yönetmelikleri başta olmak üzere yasalara bağlı olan yönetmeliklere aykırı faaliyetlerde bulunmak amacıyla kullanılamaz.

- Üniversitenin ağ hizmetleri akademik ve idari işlemlerin görülmesi amacıyla verilmektedir. Diğer kullanımlar, ancak bu kullanım gereksinimleri karşılandıktan sonra arta kalan zaman ve kapasite boyutlarında gerçekleştirilebilir.

- Üniversitenin ağ alt yapısı ve bilgisayar ağı üzerinde yer aldığı Ulusal Akademik Ağ (ULAKNET) ve diğer ulusal ve uluslararası ağların kullanım politikalarına, bilişim kaynaklarını kullanan bütün birimlerin ve bütün kullanıcıların uyma ve bu bağlamda gerekli önlemleri alma zorunluluğu vardır.

- Ağ ekipmanları Bilgi İşlem Daire Başkanlığının yetkilendirdiği kişiler tarafından erişilebilecek ve yönetilebilecektir. Kurum ağına ve ağ ekipmanlarına yetkisiz erişim yasaktır.

- Kurum ağı, sadece kurum bilgisayarları, ağ ekipmanları ve mobil cihazlar bağlanacak şekilde yönetilmektedir. Kuruma ait olmayan bilgisayar veya mobil cihazlar kablosuz olarak (KU_Misafir) ayrı bir ağ üzerinden bağlanacaktır.

- Misafirler için özel misafir ağı, kurum ağından bağımsız özel kablosuz internet hattı oluşturulmuştur. Misafirler bu ağı kullanırken İnternet Erişimi Politikası'na uygun hareket edecektir.

- Bilgi teknolojileri ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için yedek ağ ekipmanları bulundurulacaktır.
- Ağ cihazlarının konfigürasyonları düzenli olarak ağ takip programı üzerinden yedeklenecektir.
- Uzaktan bağlantı için kullanılacak portların güvenliği sağlanacaktır.
- Ağ cihazları yılda en az 1 defa açıklık (sızma) tarama testlerinden geçirilerek zafiyetler tespit edilecek ve gerekli tedbirler alınarak güvenli hale getirilecektir.
- Kurumun bilgi teknolojileri ağı detaylı olarak takip (monitoring) ve analiz edilecektir.
- Kabin yerleri, birimlerdeki ağ alt yapısı kurulurken, internet erişiminin en verimli şekilde kullanılması, ağ alt yapısı masraflarını ve kablo mesafelerine bağlı olarak veri kayıplarının en aza indirgenmesi dikkate alınarak belirlenir. Üniversite internet kullanıcıları kabin ve kabin odalarıyla ilgili aşağıdaki kurallara uymak zorundadır.
- Bilgi İşlem Daire Başkanlığı çalışanlarının haricinde hiçbir kullanıcı kabin içerisine müdahalede bulunamaz.
- Kabinleri besleyen elektrik prizlerine, sigortalara ve kesintisiz güç kaynağına müdahalede bulunamaz.
- Kabinlerin üzerine eşya, yakınına sıvı maddeler konulması ve kabinin güvenliğini bozacak her türlü durum için ortaya çıkabilecek sorunlardan ilgili birim, fakülte, enstitü, yüksekokul veya meslek yüksekokulu sekreterliği sorumludur.
- Kabin yerleri, birimlerdeki ağ alt yapısı kurulurken, internet erişiminin en verimli şekilde kullanılması, ağ alt yapısı masraflarını ve kablo mesafelerine bağlı olarak veri kayıplarının en aza indirgenmesi dikkate alınarak belirlenir.
- Üniversitenin ağ hizmetleri kaynaklarının herhangi bir amaçla kullanım hakkı, Bilgi İşlem Daire Başkanlığı ya da Rektörlük Makamı tarafından onay verilmeden üçüncü özel veya tüzel kişilere verilemez.
- Bilgi İşlem Daire Başkanlığının bilgisi dışında ağ kurmak, aktif-pasif cihazları ağa eklemek veya kablosuz yayın yapmak kesinlikle yasaktır.

- Üniversitede kablosuz ağ kullanıcıları, ağ üzerinde kendilerine verilen kullanıcı yetkisini ve kullanıcı kodunu, şifresini kullanarak bu kaynaklar üzerinde gerçekleştirdikleri çalışmalar ve etkinlikler ile bu kaynaklar üzerinde bulundurdukları veya oluşturdukları bilgi, belge, yazılım gibi her türlü kaynağın içeriğinden ve kullandıkları kaynakların kullanım kurallarına uyulmasından şahsen sorumludur.

- Bilgi İşlem Daire Başkanlığının sağladığı güvenlik çözümleri haricinde kullanılan kişisel güvenlik çözümlerinin kullanılmasıyla birlikte oluşacak sorunlardan kişi kendisi sorumludur.

- Veri kablosu, sonlandırma ve aktarma işlemlerinde kullanılan bütün bileşenlerin (patch panel, veri prizi, patch ve drop kablolar vs.) uluslararası kablolama standartlarına uygun olarak kullanılması zorunludur.

- Kampüs içinde ve binalar arasında dolaşan fiber optik (F/O) hattının zarar görmemesi için gerekli önlemleri almak ve bu fiber ağının geçtiği yerlerde yapılan inşaat, kazı ve diğer faaliyetleri denetlemek ve oluşabilecek sorunların tamir onarımını yapmak Bilgi İşlem Daire Başkanlığının sorumluluğunda değildir.

- Cihazların ve bu cihaza bağlı ekipmanların fiziki sorumlulukları, cihazın bulunduğu yerin (bina, kat laboratuvar vs.) birim amiri ve birim amirinin belirlemiş olduğu oda ve kabin sorumlusuna aittir.

P08 UZAK BAĞLANTI POLİTİKASI

1. Amaç

Kurumun bilgi teknolojileri sistemlerine dışarıdan yapılacak olan uzak bağlantıların güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bu politika bilgi teknolojileri sistemlerine dışarıdan bağlantı yapacak bütün kurum çalışanlarını ve paydaşlarını kapsamaktadır.

3. Politika

- Uzaktan bağlantı sadece SSL VPN ile yapılmaktadır.
- Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya paydaşlar yerel ağdaki kullanıcılar ile eşit sorumluluklara sahip olacaktır.
- Kurum paydaşlarının, Uzak Bağlantı Talep Formu ile birlikte ekinde bulunan Uzak Bağlantı Politikası ve Taraf Güvenlik Politikası'nı imzalaması gerekmektedir.
- VPN kullanım hakkı verilen kişiler listelenecek ve en az yılda 1 kez düzenli olarak kontrol edilecektir.
- VPN kullanım hakkı verilen kişilerin kullanıcı hesap bilgilerini başkalarıyla paylaşması yasaktır.
- VPN kullanım yetkileri Uzak Bağlantı Talep Formuna göre tanımlanacaktır, VPN hesapları formda talep edilen yetki dışında kullanılmayacaktır.
- Kurum bilgisayarları haricinde VPN bağlantısı yapılacak cihazlarda anti-virüs yazılımları kurulu ve güncel olmak zorundadır.
- Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.

P09 3. TARAF GÜVENLİK POLİTİKASI

1. Amaç

Kurumun bilgi teknolojilerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda güvenliğinin sağlanması amaçlanmaktadır.

2. Kapsam

Bu politika bütün Üniversite birimleri/çalışanları ve paydaşları (tedarikçiler, müşteriler, ziyaretçiler, bakım firmaları vb.) kapsamaktadır.

3. Politika

- Kurum paydaşları ile bilgi teknolojileri sistemlerimize veya bilgi varlıklarına müdahale, test, bakım onarım vb. amaç ile geldiklerinde Gizlilik Sözleşmesi yapılacaktır ve bulundukları sürece kurum politikalarına uygun hareket etmekle yükümlüdürler.

- Kurum paydaşları ile kuruma ait özel bilgilerin paylaşıldığı proje veya iş anlaşmaları durumunda Gizlilik Sözleşmesi yapılacaktır.

- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarımız üzerinde yapacakları çalışmaları Kastamonu Üniversitesi Bilgi İşlem Daire Başkanlığına bildirmek zorundadır.

- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına, kendilerine verilen yetki kapsamında erişim sağlayacaktır.

- Kurum paydaşları bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim yetkileri, çalışma alanlarını kapsayacak şekilde kısıtlı yetki verilecektir. İşlem logları saklı tutulacak ve çalışma bittikten sonra verilen yetkiler hemen geri alınacaktır.

- Kurum paydaşlarına bilgi teknolojileri sistemlerimize eriştikleri süre boyunca Kastamonu Üniversitesi Bilgi İşlem Daire Başkanlığı'nın belirlediği yetkili personel tarafından refakat edilecektir.

- Kurum paydaşlarına bilgi teknolojileri sistemlerimize veya bilgi varlıklarına erişim izni verilecek bilgisayarlar/mobil cihazlar için UZAK BAĞLANTI POLİTİKASI uygulanacaktır. Kurum gerekli gördüğü durumlarda herhangi bir uyarıda bulunmadan VPN bağlantı erişimlerini kesme hakkına sahiptir.

P10 KABUL EDİLEBİLİR KULLANIM POLİTİKASI

1. Amaç

Bilgi teknolojileri sistemlerine ve bilgi varlıklarına Gizlilik, Bütünlük ve Erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarını çalışanlara bildirmeyi amaçlamaktadır.

2. Kapsam

Bu politika bütün Üniversite birimleri/çalışanları ve paydaşları (tedarikçiler, vatandaşlar, ziyaretçiler vb.) kapsamaktadır.

3. Politika

- Kurumda bilgi sınıflandırması "Tasnif Dışı", "Hizmete Özel", "Özel", "Gizli" ve "Çok Gizli" olmak üzere 5'e ayrılır. Tüm bilgi, belge ve dijital dokümanlarda bilgi sınıflandırılması yapılması zorunludur.

- Kurum bilgisayarının veya cihazlarının, çalışandan alınması durumunda; çalışanın cihazlar üzerindeki kişisel verileri için erişim yetkisi istemesi halinde Üst Yönetim bilgisayar veya cihazlara erişim izni vermeme hakkına sahiptir.

- Bilgi İşlem Daire Başkanlığı'nın Gizli olarak belirlediği bütün bilgilerin gizliliğine uyulması zorunludur. Bu bilgilerin izinsiz olarak kopyalanması, çoğaltılması, paylaşılması ve iletilmesi yasaktır.

- Bütün çalışanlar, kendilerine tahsis edilmiş bilgisayar / cihazların erişim bilgilerini ve güvenliğini korumakla sorumludur ve paylaşması yasaktır.

- Çalışanların, bilgisayarından anti-virüs koruma yazılımını devre dışı bırakması yasaktır.

- Çalışanların kuruma ait bilgisayar ve cihazlarda kaynağı belli olmayan veya üretici firma tarafından kopya edilmesi yasaklanmış bir yazılımı kullanması veya kopyalaması yasaktır.

- Kuruma ait bilgisayarlara ve cihazlara lisanssız program yüklenmesi yasaktır.

- Kullanıcıların kurumun kendilerine tahsis etmiş olduğu bilgisayar, cihaz ve kurum dosya sunucusu üzerinde kuruma ait bilgi, belge, programlar ve kurumun amacı dışında dosya bulundurması veya paylaşması yasaktır.

- Donanım envanterine kaydedilmemiş cihazların tespiti halinde ilgili Birime haber verilerek cihazların envanter kaydı yapılır. Envanter kaydı olmayan cihazlar için de bu politikada geçen maddeler aynen geçerlidir.

- Kullanıcıların kurumun kendilerine tahsis etmiş olduğu bilgisayar veya cihazlar üzerinde iş amacı haricindeki programları (oyun, eğlence vb.) kullanması yasaktır.

- Kritik dokümanlara erişim yetkisi bulunan kullanıcı, doküman içeriğindeki bilginin uygun bir şekilde korunmasından sorumludur.

- Herhangi bir kişi kendine ait olmayan kritik bir doküman bulur ise bu durumu Genel Sekreterliğe bildirecektir.

- Çalışanlar, "Gizli" ve "Çok Gizli" belgeleri kilitli dolaplarda muhafaza edecektir.

- Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez. Saatler sistem tarafından otomatik olarak yönetilmektedir.

- Çalışan, taşınabilir cihazları (dizüstü, tablet, cep telefonu, harici disk vb.) güvenlik açıklarına karşı daha dikkatle korumak zorundadır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda en kısa zamanda Birim Amirine de bilgi vererek Bilgi İşlem Daire Başkanlığına haber verilmesi gerekmektedir.

- Çalışanların kurumun tahsis ettiği bilgisayar ve cihazları kendisi dışında herhangi bir kimseye (iş arkadaşları, aile bireyleri vb.) kullandırması ve paylaşması yasaktır.

- Kritik öneme sahip bilgiler dosya sunucusunda (K:/ klasörü üzerinde yetkilendirilmiş alan) saklanacaktır, kişisel bilgisayarlarda tutulmayacaktır.

- Kullanıcıların program yükleme ve bilgisayarındaki diğer iş talepleri; ÜBYS destek modülü üzerinden gerçekleştirilecek ve Bilgi İşlem Daire Başkanlığı tarafından yönetilecektir.

- Tamire verilmek üzere kurum dışına çıkartılıp üçüncü parti firmaya teslim edilecek bilgisayar/cihazlarda kurumsal bilgi bulunmayacak, bu veriler güvenli sil yöntemleriyle silinecektir.

- Bilgi İşlem Daire Başkanlığı'na arıza için verilen cihaz Başkanlık ilgili birimi tarafından kayıt altına alınır. Aynı şekilde Birimler de Bilgi İşlem Daire Başkanlığı ya da üçüncü parti firmaya teslim edilecek cihazlarını kayıt altına alırlar. Bu kayıtlarda en az cihaz marka model bilgisi, seri numarası, arıza tarihi, arızaya müdahale eden personel bilgisi, cihaz sahibi ve birimi bilgisi tutulur.

- Dijital varlıkların imhasında "Güvenli Sil" işlemi uygulanır.

P11 TEMİZ MASA TEMİZ EKRAN POLİTİKASI

1. Amaç

Çalışanların mesai saatleri içi veya dışında görevleri gereği kullandığı bilgi/bilişim ürünlerinin (yazılı doküman, belgeler, formlar, bilgisayarlar, e-posta vb.) yetkisiz erişim veya uygunsuz kullanımı sonucunda oluşabilecek riskleri ortadan kaldırmayı amaçlamaktadır.

2. Kapsam

Bu politika kurumun bütün çalışanlarını kapsamaktadır.

3. Politika

- Kurum çalışanları, çalışma masasından ayrıldığında basılı doküman ya da taşınabilir depolama aygıtları üzerinde tutulan bilgiler güvenlikli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklayacaktır.

- Her türlü faks, fotokopi, yazıcı vb. cihazlar üzerinde yetkisiz erişimlere karşı belge, doküman vb. bırakılmayacak ve sürekli kontrol edilecektir.

- Bilginin kullanıldığı sistemler (sunucular, kamera DVR cihazları, bilgisayar, cep telefonları vb.) şifresiz kullanılmayacak ve korumasız bir şekilde bırakılmayacaktır.

- Bilgi teknolojileri sistemlerinde kullanılan kullanıcı adı ve şifreler bilgisayar veya masa üzerinde yazılı olarak bulundurulmayacaktır.

- İhtiyaç duyulmadığına karar verilen dokümanlar ve içinde bilgi bulundurulabilecek elektronik cihazlar uygun metotlarla (kağıt öğütücü, disk/disket kıyıcı, yakma vb.) imha edilecektir.

- Gizli olarak tanımlanan (sözleşme, fatura, kişisel veri içeren, şartnameler, veri dokümanları vb.) dokümanlar ve kopyaları, müsvedde olarak kullanılmayacak ve kağıt öğütücü ile imha edilecektir.

- Çalışanların kullandığı kurum bilgisayarları en fazla 5 dakika boyunca herhangi bir işlem yapılmadığında otomatik olarak kilitlenecektir. Ayrıca bu işlem **Windows + L** tuşuna basılarak anlık olarak yapılabilecektir.

- Kullanıcılar bilgisayarlarının masaüstlerindeki dosyalarını, düzenli olması için klasörler içerisinde muhafaza edeceklerdir.

P12 MOBİL CİHAZ POLİTİKASI

1. Amaç

Kuruma ait bilgi içeren mobil cihazların güvenli kullanım ve yönetimini amaçlamaktadır.

2. Kapsam

Kuruma ait bilgi içeren bütün mobil ve taşınabilir cihazları kapsar.

3. Politika

- Kuruma ait mobil cihazlar (cep telefonu, dizüstü bilgisayar, usb bellek, harddisk, tablet vb.) ilgili kişiye zimmetlenerek teslim edilmelidir.
- Her çalışan kendisine zimmetlenen cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
- Dizüstü bilgisayarlar admin yetkisi sınırlandırılarak yalnızca user yetkilendirmesi ile ilgili kişiye teslim edilir.
- Kuruma ait bilgi içeren mobil cihazlara yetkisiz müdahaleyi önlemek için kullanıcı tarafından şifre tanımlanması zorunludur.
- Kuruluş telefon hatları ve mobil cihazlar üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde iletişim kurmak, mesajlar yayınlamak ve paylaşmak yasaktır.
- Mobil cihazlar üzerinde yapılan çalışmalar güvenli alanlarda mümkünse şifreli olarak saklanmalıdır.
- Kuruma ait bilgi içeren/işleyen mobil cihazların tamamında anti-virüs kullanımı zorunludur. Anti-virüsün güncel tutulmasından kullanıcı sorumludur.
- Tüm mobil cihazların yazılımları güvenlik açıklıklarına karşı en güncel haliyle kullanılır.
- Demirbaş sistemine kayıtlı mobil cihazlara kontrolsüz yazılım yüklenmemesi ve/veya çalıştırılmaması, lisanssız yazılım kullanılmaması esastır.
- Çalışanlar kişisel mobil cihazlarını “Gizli” ve “Çok Gizli” seviyesindeki Kurum iş ve işlemlerinde kullanamaz.
- Kurumun tahsis ettiği mobil cihazların kendisi dışında herhangi bir kimseye (iş arkadaşları, aile bireyleri vb.) kullandırılması ve paylaşılması yasaktır.

- Mobil cihazlarda ne tür bilgiler saklandığının farkında olunmalı ve kuruma ait bilgiler mümkün olduğunca mobil cihazlar üzerinde bulundurulmamalıdır.

P13 VERİTABANI GÜVENLİK POLİTİKASI

1. Amaç

Kurumun veri tabanı sistemlerinin güvenli kullanım ve yönetimini amaçlamaktadır.

2. Kapsam

Bütün veri tabanı sistemlerini kapsar.

3. Politika

- Veri tabanında kritik verilere her türlü erişim işlemlerinin (okuma, değiştirme, silme, ekleme) log kayıtları tutulacaktır. Log kayıtlarına, Bilgi İşlem Daire Başkanlığı'nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
- Veri tabanı bulunan sunuculara, Bilgi İşlem Daire Başkanlığı'nın yetkilendirdiği kişiler dışında erişim yapılması yasaktır.
- Veri tabanı sunucularına bağlanma yetkisine sahip kullanıcılar sadece kendi kullanıcı adı ve şifresi ile bağlantı yapacaktır.
- Sunucularda bulunan veri tabanlarının kritiklik seviyelerine göre yedekleri alınacaktır.
- Veri tabanı sunucuları fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.
- Veri tabanlarında yapılacak bakım onarım ve güncelleme çalışmalarından önce ilgili birimlere duyuru yapılacaktır.
- Veri tabanı bulunan medyalar (harici disk, usb bellek vb.) kurum dışına çıkarılmayacaktır.
- Veri tabanlarına kurum dışından erişimler Uzak Bağlantı Politikası'na uygun şekilde yapılacaktır.
- Veri tabanı sunucularının kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak kontrol edilecektir.
- Veri tabanlarına kurum dışından erişim sağlayan firmalar ile Bilgi İşlem Daire Başkanlığı arasında Gizlilik Sözleşmesi imzalanacaktır.

P14 YAZILIM TEMİNİ ve GELİŞTİRME POLİTİKASI

1. Amaç

Kurumun yazılım temini ve geliştirme ihtiyacının güvenli yönetilmesini amaçlamaktadır.

2. Kapsam

Bütün yazılım temini ve geliştirmelerini kapsar.

3. Politika

- Bilgi İşlem Daire Başkanlığı, kaynak yönetimini sağlamak, mevcut altyapıya ve kullanım amacına uygun yazılım projeleri gerçekleştirmek ile yükümlüdür.
- Yazılım geliştirmede, ihtiyaç analizi, tasarım, geliştirme, deneme ve onaylama safhalarını içeren iş planı kullanılacaktır, teknik hatalara istinaden yapılan geliştirme istekleri Bilgi İşlem Daire Başkanlığı E-Posta adresi (bidb@kastamonu.edu.tr) üzerinden yönetilecektir.
- Kurum genelinde kullanılacak yazılımların (geliştirilen veya satın alınan) kanunlarla belirli olan şartları sağlaması zorunludur. Bu konuda Bilgi İşlem Daire Başkanlığı sadece kendi onayladığı yazılımların sorumluluğunu kabul etmektedir. Birimlerin Bilgi İşlem Daire Başkanlığı'nın onayını almadan yaptıkları yazılım alımlarında ya da kullanımlarında ise sorumluluk birimlere aittir.
- Kurum genelinde kullanılacak olan yazılımlarda Bilgi İşlem Daire Başkanlığı tarafından onaylanmış yazılımların (geliştirilen veya satın alınan) kullanılması öncelik arz etmektedir.
- Yeni alınmış veya revize edilmiş bütün yazılımlar Bilgi İşlem Daire Başkanlığı tarafından test edilecek ve onaylanacaktır.
- Kuruma ait yazılımlar Varlık Envanteri Listesine eklenecek ve takip edilecektir.

P15 DEĞİŞİM YÖNETİMİ POLİTİKASI

1. Amaç

Kurumun bilgi teknolojileri sisteminde yapılması gereken yazılımsal ve donanımsal değişikliklerde süreklilik ve güvenliği sağlamayı amaçlamaktadır.

2. Kapsam

Bu politika kurumun bütün çalışanlarını ve Kurum varlık envanterine kayıtlı cihazları kapsamaktadır.

3. Politika

- Yazılımsal ve donanımsal değişiklik talepleri ÜBYS destek modülü üzerinden gerçekleştirilecek ve Bilgi İşlem Daire Başkanlığı tarafından yönetilecektir.
- Yazılımsal ve donanımsal değişiklikler yapılmadan önce, bu değişiklikten etkilenecek bütün sistem ve uygulamalar belirlenerek ilgili kişilere bilgi verilecektir.
- Yazılımsal ve donanımsal değişikler gerçekleştirilmeden önce değişikliğin yapılacağı sistemlerin yedekleri ilgili kullanıcı personel tarafından alınacak olup, teknik personel sürece dahil edilmeyecek, sorumlu tutulmayacaktır.
- Sistemlerde yapılacak değişikliklerde ilgili üretici tarafından onaylanmış güncellemeler kullanılacaktır.
- Yazılımsal ve donanımsal değişiklikler, sisteme alınmadan önce Bilgi İşlem Daire Başkanlığı veya ilgili alt birim tarafından onaylanacaktır.

P16 OLAY YÖNETİM POLİTİKASI

1. Amaç

Bilgi güvenliği olaylarının kayıt altına alınması ve yönetilmesini amaçlamaktadır.

2. Sorumlular

Bu politikanın uygulanmasından bütün personel sorumludur.

3. Politika

- Bilginin gizlilik, bütünlük ve erişilebilirlik açısından zarar görmesi, bilginin son kullanıcıya ulaşana kadar bozulması, değişikliğe uğraması ve başkaları tarafından ele geçirilmesi, yetkisiz erişim gibi güvenlik ihlali durumları düzenli olarak kayıt altına alınacaktır. Yaşanan olaylar Bilgi Güvenliği Olay Yönetimi Politikası'na göre yönetilecektir.

- Yaşanan Bilgi Güvenliği olayları Bilgi İşlem Daire Başkanlığı Siber Olaylara Müdahale Ekibi'ne (SOME) (some@kastamonu.edu.tr) e-posta ile bildirilecektir.

- Bilgi Güvenliği olayının kaynağı SOME tarafından araştırılacak ve olayın önemlilik seviyesine göre müdahale edilecektir.

- Bilgi güvenliği olayı kayıtları (log, fotoğraf, video vb) SOME tarafından saklanacaktır.

- Yaşanan Bilgi Güvenliği olayları cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa disiplin yönetmeliğini uygulayabilir veya yasa uygulayıcısı ile işbirliği yapabilir.

- Bilgi Güvenliği olayları analiz edilerek tekrarlanmaması için gerekli önlemler alınacaktır.

P17 KRİPTOGRAFİK KONTROLLER POLİTİKASI

1. Amaç

Bilgi varlıklarının saklandığı sistemlerin ve bilgi varlıklarının transferinin gizliliğini veya bütünlüğünün şifreleme yöntemleri ile korunması amaçlanmaktadır.

2. Kapsam

Bu politikanın uygulanmasından bütün personel sorumludur.

3. Politika

- Gizli olarak ifade edilen bilgi varlıklarının paylaşımında güçlü şifreleme algoritması kullanılacaktır. Gizli bilgi varlıklarının paylaşımı sırasında şifreli sıkıştırma programı(7zip, Winrar, Winzip vb.) ile sıkıştırılarak şifrelenecektir.
- Mobil cihazlardaki verilerin korunmasında şifre kullanılmalıdır.
- E-posta hesabı kurulu akıllı telefonlarda telefon kilidi kullanılması zorunludur.
- Tanımlanan şifreler belirli aralıklarla değiştirilmelidir.
- KBTS hesap şifreleri kolay tahmin edilmeyen karmaşık şifreler olmalıdır.
- Misafirlerin internet kullanımı için misafir ağına bağlanılırken şifre kullanılır.
- Kurumun e-posta sistemi SSL serfikası ile şifrelenir.
- Kurumdaki çalışanların kullandıkları E-İmza ve KEP vb. sistemler ile veriler şifreli şekilde imzalanmalıdır.

P18 KAMERA POLİTİKASI

1. Amaç

Üniversite bünyesindeki IP kameralar ile oluşturulan verilerin, belirli bir süre saklanması ve muhafazası konusunda gerekli önlemleri almaktır.

2. Kapsam

Bu politika kurumun bütün çalışanlarını kapsamaktadır.

3. Politika

- Üniversitemiz bünyesinde IP kameraların kayıtlarını tutmak için NVR (Network Video Recorder) sunucuları kullanılmaktadır.
- Bütün IP kameraların kayıtları en az 20 gün sunucularda tutulmaktadır.
- Bilgi İşlem Daire Başkanlığı Merkez Kampüste bulunan IP kameraların bakımlarını, onarımlarını kendi bünyesindeki personeli yapacaktır. Bunun dışındaki analog veya IP kameralar bina yöneticisi sorumluluğundadır.
- Merkez Kampüs haricindeki kameralar için veri saklama ya da bakım hizmeti birimlerin sorumluluğundadır. Bu kameralar ve kayıt cihazları için de Bilgi Güvenliği Uygulama Politikaları uygulanır.
- Üniversite bünyesindeki kameralar tarafından alınan video kayıtlarının canlı görüntülerinin izlenmesi İdari ve Mali İşler Daire Başkanlığı'na güvenlik amirliği sorumluluğundadır.
- Bilgi İşlem Daire Başkanlığı yeni kamera kurulumları için gelen talepleri güvenlik amirliğinin uygun görmesi ve ilgili birim talebi doğrultusunda yapmaktadır.
- Personelin geçmişe dönük kamera kayıt izleme talepleri için güvenlik amirliğine başvurması gerekmektedir. Güvenlik amirinin uygun görmesi ile Güvenlik Merkezi'nde izlenilmesine izin verilebilir. Kayıt izleme talepleri tutanak veya formla kayıt altına alınır.
- Görüntü kayıtları Üniversite yönetiminin izni ve talebi ile resmi belge karşılığında verilir. Kayıtların depolanacağı alanı talepte bulunan kişi veya kurum sağlar.
- Görüntü talebinde bulunan ve talebi karşılanan kişi/kurum KVKK kapsamında hareket edecek, yasa koyucu ve uygulayıcı dışında kalan 3. taraflarla paylaşmayacaktır.

- Güvenlik görevlileri, güvenlik kamerası izleme noktalarını Bilgi İşlem Daire Başkanlığının hazırladığı Bilgi Güvenliği Uygulama Politika kuralları dâhilinde kullanabilir.

- Güvenlik görevlileri, güvenlik amirliği tarafından belirlenen sorumlusu olduğu noktanın kendimesai saati içinde (bina, nizamiye, spor salonu vs.) güvenlik kameralarını izleyebilir.

- Güvenlik görevlileri, güvenlik kamerası görüntülerini, güvenliği sağlama amacı ile izler, üçüncü şahıslara izletemez, hiçbir şekilde kayıt altına alamaz, kopyalayamaz ve paylaşamaz.

- Güvenlik görevlileri, güvenlik kamerası izleme yazılımına Bilgi İşlem Daire Başkanlığının izni dışında müdahale edemez ve üçüncü şahısların müdahalesine izin veremez.

- Bilgi İşlem Daire Başkanlığı güvenlik kamerası izleme noktalarının amacı dışında kullanıldığını ve Anayasanın 20. maddesindeki "özel hayatın gizliliği" ve "kişisel verilerin korunması" hükmünün gözetilmediğini tespit ettiğinde, birim yetkililerine ve Üniversite yönetimine bilgi vererek gerekli tedbirleri alır.

P19 YEDEKLEME POLİTİKASI

1. Amaç

Üniversite ağı ve cihazları üzerinde oluşturulan, kullanılan ve devamlılığı gerekli görülen verilerin saklanması ve muhafazası konusunda gerekli önlemleri almaktır.

Bu politikanın uygulanmasından bütün personel sorumludur.

2. Kapsam

Bilgi İşlem Daire Başkanlığının kontrolünde olan ve Üniversite bünyesinde oluşturulan verilerin (yedekleme üniteleri ve sunucularda) güvenli olarak yedeklenmesi, gerektiğinde kullanıma açılması ve ihtiyaç sonunda silinmesi için gerekli yöntemlerin belirlenmesini tanımlar.

Üniversite bünyesinde yedekleme Bilgi İşlem Daire Başkanlığının kurmuş olduğu sistem ve sanal sunucuların veri yedeklerini kapsar.

3. Politika

- Bilgi İşlem Daire Başkanlığı kendi kontrolünde olan ve gerekli gördüğü bütün cihazların, sistemlerin, ağların vs. kayıtlarını kendi belirlediği süre içerisinde düzenli olarak almaktadır. Belirlenen zaman boyunca saklamakta ve belirlenen zaman dolduğunda da silmektedir.

- Bilgi İşlem Daire Başkanlığı kontrolünde olmayan kullanıcıların kullandığı cihazlara ve sistemlere vs. ait olan kişisel ve özel verilerin yedeklenme ve saklanma işlemlerinden kullanıcı kendisi sorumludur. Bilgi İşlem Daire Başkanlığı herhangi bir veri kaybından ya da kaybolan verilerin kurtarılmasından sorumlu tutulamaz.

- Üniversitede elektronik ortamda veriyi üretme ve/veya yönetme ile görevlendirilen bütün personel sorumludur.

- Üniversite bünyesinde kullanılan sunucu ve sistemlerin düzenli aralıklarla önem sırasına göre yedekleri alınmalıdır.

- Sunucu yedeklerinin belirlenen yedekleme süre periyotları ölçüsünde veri kaybı kabul edilebilir. (24 saatte bir yedeği alınan sunucunun arızalanması durumunda 24 saatlik veri kaybı kabul edilebilir)

P20 WEB SAYFASI TAHSİSİ POLİTİKASI

1. Amaç

Kastamonu Üniversitesinin, kurumsal kullanıcılarına sağladığı alan adlarının kullanım yönergesini oluşturmak ve kullanım ilkelerini belirlemek.

2. Kapsam

Bu politika kuruma ait web sayfası kullanan bütün birimlerini/çalışanlarını kapsamaktadır.

3. Politika

- Kastamonu Üniversitesi, alan adı (subdomain) hizmetini, yalnızca kurum bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci grupları, konferanslar, toplantılar, sempozyumlar, kongreler, çalıştaylar, paneller vs. gibi kurumsal yapılara sağlamaktadır.

- Üniversite bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci grupları, konferanslar, toplantılar, sempozyumlar, kongre, çalıştay, panel vs. gibi yapılar üniversitenin kurumsal kimliğinin bozulmaması için Bilgi İşlem Daire Başkanlığı tarafından sağlanan web sitelerini kullanacaklardır.

- Rektörlük oluruyla kendi web sitesini oluşturmuş olan birimlerin sitelerine ise Bilgi İşlem Daire Başkanlığı tarafından barındırma hizmeti dışında herhangi bir destek verilmeyecektir. Sunucu ve sistem güvenliği birimin kendi sorumluluğu altındadır. Oluşabilecek bütün yasal ve teknik sorunlardan ilgili birim ve web site yöneticisi sorumlu olacaktır.

- Alan adı (subdomain) alma talepleri, Bilgi İşlem Daire Başkanlığına https://bidb.kastamonu.edu.tr adresinde bulunan web sayfası istek formunun talebi yapan kurumsal birimin yöneticisi tarafından imzalanması ve bir görevli personel ataması yapılarak başvurmasıyla yapılır.

- Alan adı ve site içeriği ile ilgili olarak olası hukuki süreçlerden ve sorunlardan adına web alanı tahsis edilen kullanıcı sorumludur.

- Üniversitemiz bünyesinde Bilgi İşlem Daire Başkanlığı tarafından açılan web sitesi ve alt alanlar (subdomain) dışında yapılan web sitesi veya alt alanların (subdomain) yönlendirilme taleplerine destek verilmemektedir.

- Üniversite ve öğrenci toplulukları tarafından organize edilen veya katılımda bulunulan ulusal/uluslararası etkinlik ve organizasyonlar için verilen alan adresleri ilgili birim ya da topluluklardan resmi yazı ile talep gelmesi üzerine açılmaktadır.

- Kullanıcı web kota bilgisi sadece Bilgi İşlem Daire Başkanlığının verdiği alanla sınırlıdır. Sonradan yapılan kota artırım talepleri ise Bilgi İşlem Daire Başkanlığının kaynak durumuna göre, gerekli görülmesi ve uygun ortamın bulunması durumunda sağlanacaktır.

- Web sitesi ve alt alan adı tahsis edilen birim, personel, etkinlik ve organizasyonlar yayınladıkları web sitelerinde Üniversite Bilgi Güvenliği Uygulama Politikalarına uymak zorundadırlar. Kullanıcı, web alanı hizmetinden faydalanırken Bilgi İşlem Daire Başkanlığı tarafından yayınlanan her türlü ihtar ya da bildirime uymayı beyan, kabul ve taahhüt eder. Kullanıcı, almış olduğu web alanı hizmetini üçüncü kişilere her ne ad altında olursa olsun kullandıramaz.

- Kullanıcı, kişisel web alanında barındırdığı bütün dosya, doküman ve programlardan, web sitesi ve eposta hizmetleri ile kullanacağı ve faydalanacağı bütün işlemlerden kendisinin sorumlu olduğunu; söz konusu veri, bilgi, beyanların yasalara aykırılığından ve web alanında barındırdığı web sayfası ya da programların güvenlik açıkları nedeniyle başka bir sunucuya yapılacak saldırıdan doğabilecek bütün hukuki ve cezai sorumluluğu kendisi karşılamayı kabul ve taahhüt eder. Bu konuda doğabilecek sorunlardan Bilgi İşlem Daire Başkanlığına herhangi bir sorumluluk yüklenemez.

- Bilgi İşlem Daire Başkanlığı kullanıcıların hizmet aldığı merkezi sunucular üzerinde herhangi bir zamanda teknik değişiklikler yapma hakkına sahiptir. Bu değişiklikleri önceden kullanıcılara bildirebileceği gibi, anlık olarak yapılabilecek değişikliklerin önceden duyurulamaması da mümkün olabilir. Kullanıcılar oluşacak veri kaybı vs. gibi konularda herhangi bir hak talep edemez.

- Bilgi İşlem Daire Başkanlığı, birimlerin kendi imkânları ile hazırlamış oldukları web siteleri için güvenlik testi yapmaz, güvenlik açıklarını kontrol etmez, kurulan eklentilerinin güvenlik açıklarını test etmez, doğrulamaz, ciro etmez veya kullanıcı tarafından yapılmış sayfalar için herhangi bir şekilde bir sorumluluk almaz.

- Bilgi İşlem Daire Başkanlığı, birimlerin kendi imkânları ile hazırlamış oldukları web sitelerinde güvenlik açığı bulunmasından dolayı hizmet alan diğer kullanıcılarına veya üçüncü şahıslara herhangi bir şekilde zararlı olduğuna karar verdiği durumlarda hizmeti kesebilir veya müdahale edebilir.

- Bilgi İşlem Daire Başkanlığı hukuka aykırı fiil ve eylemleri öğrendiğinden itibaren kullanıcıya haber vermeden kullanıcı hesaplarını geçici veya sürekli olarak kapatmak veya silmek hakkına sahiptir.

- Bilgi İşlem Daire Başkanlığı, sağladığı hizmet içerisinde bulunan kullanıcı verilerinin hatalı kullanımlarından, veri içeriklerinden, e-posta ile kullanılan bütün verilerden doğabilecek hiç bir maddi veya manevi zararlardan sorumlu tutulamaz. Bu verilerin yedekleme ve saklama yükümlükleri kullanıcıya aittir.

- Bilgi İşlem Daire Başkanlığı yedekleme işlemlerini Bilgi Güvenliği Uygulama Politikalarında belirtilen Yedekleme Politikası'na uygun olarak yapacaktır.

- Bilgi İşlem Daire Başkanlığı bakım işlemlerini kendi bünyesinde hazırlamış olduğu günlük ve haftalık bilişim sistemleri kontrol listeleri ile sistem kontrollerini düzenli olarak yapacaktır. Bu kontroller sırasında sorun tespit edilmesi durumunda sorun ile ilgili olay kayıt raporu formunu doldurarak gerekli müdahaleyi yapacaktır. Bu formlar Bilgi İşlem Daire Başkanlığı bünyesinde idari amirlerce onaylanarak Bilişim Sistemleri Olay Kayıt Kütüğünde kayıt altında tutulacaktır.

- Bilgi İşlem Daire Başkanlığının kontrolü dışında oluşturulmuş web sayfalarının içeriği üzerinde herhangi bir sorumluluğu yoktur. Bu sayfaların içeriğini kontrol ve takip etmez; bu sayfaların içeriği ile ilgili güvence sağlamaz.

- Bilgi İşlem Daire Başkanlığı hiçbir durumda, doğrudan veya dolaylı olarak, bu sayfalarda sunulan içeriğin kullanımı veya referans gösterilmesi ile ilgili oluşabilecek veya oluştuğu iddia edilebilecek sorun veya zararlardan sorumlu tutulamaz.

- Bilgi İşlem Daire Başkanlığı web programlama konusunda sadece gelen taleplere göre Üniversite bünyesindeki fakülteler, enstitüler, yüksekokullar, meslek yüksekokulları, birimler, bölümler, müdürlükler, koordinatörlükler, öğrenci grupları, konferanslar, toplantılar, sempozyumlar, kongreler vs. gibi kurumsal yapılara ve gruplara gerekli gördüğü takdirde web yazılım desteği sağlayacaktır.

P21 ERİŞİM KONTROL POLİTİKASI

1. Amaç

Bu politikanın amacı; Kastamonu Üniversitesi'ne ait bilgi ve bilgi işleme tesislerine erişimi kısıtlamak, yetkili kullanıcı erişimini temin etmek, sistem ve hizmetlere yetkisiz erişimi engellemek, Kastamonu Üniversitesi tarafından yönetilen bilişim sistemlerine yapılacak uzaktan erişimlerin yönetim esaslarını açıklamaktır.

2. Kapsam

Bu politika, Kastamonu Üniversitesi'ne bağlı Yönetim Birimlerinde kullanılan bilgi sistemleri ve ağlar ile ilgili erişim kontrol faaliyetlerini kapsamaktadır.

3. Politika

3.1. Erişim Kontrol Politikası (TS ISO 27001:2013 EK A-9.1.1)

İş uygulamaları, sistemler ve ağlar üzerinde tanımlanacak erişim hakları verilirken aşağıdaki hususlar dikkate alınır;

- Dağıtılmış ve ağ oluşturulmuş çevre içindeki tüm olası bağlantı hakları için erişim haklarının yönetimi belirtilir,
- Erişim Politikası, "açıkça izin verilmedikçe her şey yasaklanır" kuralı temel alınarak belirlenir. İş ihtiyacı sebebiyle izin verilmedikçe tüm erişim hakları "Reddet" olarak ayarlanır,
- Kastamonu Üniversitesi iş uygulamaları üzerinden bilgiye erişim hakları, iş ve güvenlik gereksinimlerine uygun olarak ve "Bilmesi Gereken" ve "Kullanması Gereken" prensibine uygun olarak verilir,
- Bilgi veya sistemlere erişimlerde, veri koruma ve gizlilik ile ilgili mevzuata uyulur.
- Erişim hakları ile bilgi sınıflandırılması arasında tutarlılık olur,
- İş uygulaması sahibinin, uygulamaya erişim yetkisini düzenleme hakkına sahip olduğu durumlarda, erişim güvenliğinde oluşabilecek ihlallerden varlık sahibi sorumludur,
- Erişim kontrol rollerinin birbirinden ayrılması gerekir; örneğin, erişim talebi, erişim yetkilendirmesi, erişim yöneticisi, vb.

- Erişim taleplerinin resmi yetkilendirilmesi için gereksinimler bu politikanın Madde 3.2 ve Madde 3.3'üne göre yapılır,
- Erişim haklarının periyodik gözden geçirilmesi için gereksinimler Madde 3.3'e göre yapılır,
- Erişim haklarının kaldırılması Madde 3.8'e göre yapılır,
- Kullanıcı kimlik bilgileri ve gizli kimlik doğrulama bilgileri kullanımı ve yönetimi Madde 3.7'ye göre yapılır,
- Ayrıcalıklı erişim rolleri Madde 3.5'e göre yapılır,
- Kastamonu Üniversitesi varlıklarına erişim yetkileri yürürlüğe girmeden önce, özel onaya gerek duyan ve duymayan kurallar Bilgi İşlem Daire Başkanlığı tarafından belirlenir.

3.2 Ağlara ve Ağ Hizmetlerine Erişim (TS ISO 27001:2013 EK A-9.1.2)

- Kastamonu Üniversitesi iletişim ağları iş gereksinimleri ve organizasyonel olarak fiziksel ve mantıksal yapılara ayrılır. Mantıksal yapılar arasında gerekli güvenlik geçiş kontrolleri uygulanır.
- Etki alanı (domain) üyesi olmayan kullanıcıların ağ erişimleri engellenir.
- Paydaşlardan İnternete erişim talebi oluştuğunda, TC kimlik numarası, Ad, Soyad, Doğum Tarihi ile kurum Kablosuz Misafir Ağı'na erişim sağlanabilir.
- Misafir Ağlarından Kastamonu Üniversitesi yerel ağlarına doğrudan erişimler engellenir.
- Kullanıcılar varsayılan olarak standart kullanıcı erişim yetkisinin yanı sıra kendi bölüm/proje ağındaki (VLAN) diğer sunucu ve bilgisayarlara ağ erişim yetkisi Bilgi İşlem Daire Başkanlığı tarafından verilir.
- Kullanıcılar Kastamonu Üniversitesi'ne ait bilgisayarlarını, Kastamonu Üniversitesi bilgisayar ağlarına erişim yetkisi olmayan kişilere kullandırmaz.
- Kastamonu Üniversitesi bilgisayar ağına, yetkisiz kişiler tarafından modem, kablosuz erişim noktası, anahtarlama cihazı veya HUB gibi cihazlar bağlanmaz. Bağlanması durumunda bağlanan cihaz karantinaya alınır.
- Ağ üzerindeki bilgi akışının doğru yönetilebilmesi için gerekli olan yerlerde "Erişim kontrol listeleri" tanımlanır.

3.3 Kullanıcı Kaydetme ve Silme (TS ISO 27001:2013 EK A-9.2.1)

3.3.1 Üniversite Bilgi Yönetim Sistemine Kayıt Etme ve Silme

- Göreve yeni başlayan (akademik ve idari), görevde olan ve dışarıdan ders veren öğretim elemanı kullanıcı hesaplarının açılması süreci Personel Daire Başkanlığı tarafından kişilerin kimlik ve pozisyon bilgilerinin ÜBYS'ye kaydedilmesi ile başlar.

- Personel Daire Başkanlığı tarafından ÜBYS'ye kaydedilen kişiler (akademik ve idari) ilgili birime e-posta istek başvurusunda bulunur. Kişilere açılan e-posta hesapları ÜBYS'de kullanıcı adı olarak belirlenir. Sisteme kayıtlı olan cep telefonuna (GSM) kişinin kullanıcı adı ve şifresi ÜBYS Birimi tarafından SMS olarak gönderilir.

- Kullanıcı hesabıyla yapılan ilk giriş sonrasında kullanıcı hesabının parolası kullanıcı tarafından değiştirilmesi zorunlu kılınmıştır.

- Kurumumuzdan ilişiği kesilen ÜBYS kullanıcıları (akademik ve idari) Personel Daire Başkanlığı tarafından pasif durumuna çekildiğinde, ÜBYS'ye girişleri de otomatik olarak pasif duruma gelir.

- Dışarıdan ders veren öğretim elemanı kullanıcılarının hesapları Personel Daire Başkanlığı tarafından sisteme eklenmesinin akabinde açılır ve devamında Öğrenci İşleri Daire Başkanlığı tarafından ders görevlendirilmesi yapılır. Görevlendirmeler dönemlik yapılır ve dönem sonunda hesap pasife otomatik olarak çekilir. Yeni dönemde görev süresi devam etmesi halinde ÜBYS Birimi tarafından verilen kullanıcı bilgisi ile sisteme giriş yapılır.

- ÖSYM tarafından Üniversitemize yerleştirilen öğrencilerin bilgileri Öğrenci İşleri Daire Başkanlığı ile ilgili kurum tarafından paylaşılmasının akabinde, ÜBYS Birimi tarafından tek seferde toplu olarak kullanıcı adı okul numarası, şifresi de T.C. kimlik numarası olarak oluşturulur.

- Öğrencilerin sisteme ilk giriş yapmasının akabinde kullanıcı hesabının parolası öğrenci kullanıcısı tarafından değiştirilmesi zorunlu hale getirilmiştir.

- Öğrenciler, Üniversitemizden mezun olması akabinde hesapları silinmez ve aynı kullanıcı adı ile ÜBYS altında bulunan Mezun Öğrenci Takip Sistemi modülüne giriş yapmaya devam eder, ayrıca sistem üzerinden e-imzalı öğrenci belgesi ve transkript almaya devam edebilmektedirler.

3.3.2. E-posta Sistemine Kayıt Etme ve Silme

- Bilgi İşlem Daire Başkanlığına e-posta istek formu ile başvuru yapılır.
- Kurum çalışanlarının e-posta hesapları isimlerinin baş harfi ve soy isimlerinin tamamı olacak şekilde açılır. Şifreleri T.C. kimlik numarası olarak belirlenir. Şayet kullanıcı adı Üniversitemiz sisteminde daha önce kullanılmışsa personelin e-posta istek formunda belirttiği diğer kullanıcı adı seçeneklerinden sırasıyla uygun olanı tanımlanır.
- Yeni kayıt yapılan öğrencilerin e-posta hesapları, tüm kayıt işlemlerinin tamamlanmasının ardından toplu olarak açılır.
- Birimlere ait olan kurumsal e-posta hesapları, ilgili yönetici onayı ve Bilgi İşlem Daire Başkanlığına gönderilecek üst yazı sonrasında açılır. E-posta hesap bilgileri ilgili yöneticinin belirlediği tek bir çalışana verilir. Hesabın güvenliğinden bu çalışan sorumludur.
- Kurum çalışanı, hizmet alımı ile Üniversitemizde görevlendirilen ve dışarıdan ders veren öğretim elemanları iş bitiş tarihlerine göre kullanıcı hesaplarının kapatılması için ilgili birime talepte bulunulur.
- Talepte bulunulmamış e-posta adresleri için her ayın ilk haftası Personel Daire Başkanlığı tarafından ilgili birim bilgilendirilir. İlgili birim bilgilendirildiğinde e-posta hesapları "disabled" yapılır.
- Kurum'dan ayrılan çalışanların kullanıcı hesapları geçmiş kayıtların takibi nedeni ile silinmez, etkisiz (disable) hale getirilerek tanımlı olduğu sistemlerde yetkisiz kılınır. Öğrencilerin e-posta hesapları ise kurumdan ayrıldıktan 2 sene sonra silinir.

3.4 Kullanıcı Erişimine İzin Verme (TS ISO 27001:2013 EK A-9.2.2)

- “Erişim Kontrol Politikası” başlığı Madde 3.1’de belirtilen kurallar uygulanır.
- Kullanıcılar, kullanıcı girişi yapmadan herhangi bir uygulamaya veya bilgiye erişemez.
- Kullanıcılar, bilgi sistemleri kaynaklarına erişim için, ÜBYS birimine Destek Talep Modülü üzerinden talep oluşturması gerekmektedir. Birimin onayı ile yetki tanımlanır.

3.5 Ayrıcalıklı Erişim Haklarının Yönetimi (TS ISO 27001:2013 EK A-9.2.3)

- Bilgi İşlem Daire Başkanlığı sorumluluğundaki sistemlere ve uygulamalara yönetici yetkilerine sahip kullanıcı erişimleri Bilgi İşlem Daire Başkanlığı Görev Dağılım Listesi ve/veya kullanılan araç üzerinde tanımlı rollere uygun olarak tahsis edilir.
- Ayrıcalıklı erişim hakları çalışan sayısı mümkün oldukça kısıtlanır.
- Yönetici hakları, çalışan yedekliliği ve görevlerin ayrılığı ilkesi göz önünde bulundurularak tanımlanır.
- Üniversitemiz birimlerinden gelen ayrıcalıklı yetki talepleri ÜBYS Destek Talep Modülü veya EBYS üzerinden talep edilir. Bilgi İşlem Daire Başkanlığı tarafından incelenir, uygun görülmesi halinde ilgili birim ayrıcalıklı hesap tanımlamasını yapar.
- İlgili birim sorumluluğunda olan sistemlere ve uygulamalara ait parolalara, sadece ilgili sistemin operasyonel yönetiminden sorumlu yönetici haklarına sahip kullanıcılar erişebilir.
- Yönetici işlemlerini gerçekleştiren kişiler, sadece yönetimsel haklar gerektiren işler için yönetim hesaplarını kullanır. Sistem yöneticileri diğer işlerde kendileri için tahsis edilen yetkili kullanıcı hesaplarını kullanır.
- Yönetici hesaplarında yapılan işlemlere ait yönetici (admin) hareketleri kayıt altına alınır.
- Sunucuların, ağ cihazlarının ve istemci bilgisayarlarının yerel yönetici hesaplarına ayrıcalıklı hesap yönetimi yazılımı ile bağlanılmaz.
- Ayrıcalıklı hesap yönetimi yazılımı, sunucu, ağ cihazları ve istemci bilgisayarlarına tek kullanımlık veya belirli süreli şifreler ile bağlanır.
- Ayrıcalıklı hesap yönetimi yazılımı ile yapılan tüm erişimler yazılım sunucusu üzerinde loglanır ve ekran görüntü kayıtları alınır.

3.6 Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi (TS ISO 27001:2013 EK A-9.2.4)

- Kullanıcılar, kurumsal kullanıcı hesaplarına ait hassas bilgilerin (kullanıcı adı, parola, PİN numarası vb.) gizliliğini sağlamakla yükümlüdür. Bu bilgiler basılı halde, korunmasız olarak saklanmaz.

- Erişim bilgilerinin (kullanıcı adı, parola, PIN numarası vb.) gizliliğin sağlanması ve güvenlik donanımlarının (e-anahtar, manyetik giriş kartı vb.) korunması kullanıcının sorumluluğundadır.

- Kastamonu Üniversitesi kullanıcı hesaplarına kolay tahmin edilebilir ve zayıf nitelikte parolalar verilmez.

- Kastamonu Üniversitesi çalışanı ve misafir kullanıcı, kendi hesabına verilmiş erişim bilgilerini paylaşmaz, elektronik veya elektronik olmayan herhangi bir ortamda bulundurmaz.

- Kurumsal kullanıcı hesaplarına ait parolaların elektronik ortamda saklanması gerektiğinde parola yönetim araçları kullanarak gerekli güvenlik önlemleri alınması önerilir. Oluşabilecek bir güvenlik ihlalinde tüm sorumluluk kullanıcıya aittir.

- Kurumsal kullanıcı hesaplarına ait parolalar, kişisel hesaplarda (tartışma gruplarına üyelik, Sosyal Medya, Yahoo, gmail vb. e-posta hesapları) kullanılmaz.

- Bir kullanıcıya ait hesabın başkaları tarafından izinsiz kullanıldığından şüphelenilmesi durumunda, parola derhal değiştirilir ve Olay Yönetim Politikası'na göre hareket edilir.

- Kullanıcı parolaları herhangi bir otomatize giriş sisteminde (makro, function key, betik, web formları, İnternet Browser araçlarında, kaynak kod vb.) saklanmaz.

- Varsayılan ürünlerin parolaları için P04 Şifre Politikası'na göre hareket edilir.

3.7 Kullanıcı Erişim Haklarının Gözden Geçirilmesi (TS ISO 27001:2013 EK A-9.2.5)

- Kullanıcı erişim hakları, ilgili taraflarca belirli aralıklarla sistem erişim yetkisine haiz kullanıcılarla ilgili değişiklik durumları gözden geçirilerek yaşanan değişikliklerle ilgili yeni tanımlamalar ve kısıtlamalar yapılır.

- Ayrıcalıklı erişim hakları için yetkilendirmeler daha sık aralıklarla gözden geçirilir ve kayıtları tutulur.

3.8 Erişim Haklarının Kaldırılması veya Düzenlenmesi (TS ISO 27001:2013 EK A-9.2.6)

- Görev veya sorumlulukları değişen çalışan hakkında ilgili birime, ilgili yönetici tarafından resmi yazı ile bilgi verilir.

- Görevi veya sorumlulukları değişen çalışanın eski görev tanımına ait yetkilerin iptali için ilgili birim tarafından ÜBYS veya kurumsal e-posta yoluyla "Personel Unvan / Birim / Pozisyon / Rol" değişikliği talebi açılır, oluşturulan talebi yetkilendirilen personel görür.

- Görev veya sorumlulukları değişen çalışanın Unvan / Birim / Pozisyon / Rol yetkileri konu için yetkilendirilmiş personel tarafından gözden geçirilir ve gerekli düzenlemeler yapılır.

- Kastamonu Üniversitesi bilgi varlıklarına (sunucu vb.) erişim sağlayan dış tarafların Kastamonu Üniversitesi ile iş ilişkilerinin kesilmesi durumunda; ilgili yönetici ÜBYS üzerinden resmi yazı ile Bilgi İşlem Daire Başkanlığına bildirimde bulunur. Akabinde verilmiş yetkiler sonlandırılır.

- İzin, rapor ve görevlendirme gibi durumlarda, çalışanın işlerine vekâlet edecek personele hesap bilgileri verilmez. Vekalet edecek personele, ÜBYS üzerinden kişi veya ilgili birim tarafından verilen vekalet sonrası geçici erişim yetkisi verilir. Asıl çalışanın görevine dönmesi durumunda vekâlet eden çalışana verilen haklar ve erişim yetkileri iptal edilir.

3.9 Gizli Kimlik Doğrulama Bilgisinin Kullanımı (TS ISO 27001:2013 EK A-9.3.1)

- Gizli kimlik doğrulama bilgileri ilgili dokümanlar Temiz Masa Temiz Ekran Kullanım Politikası, Varlıkların Kabul Edilebilir Kullanım Politikası dikkate alınarak saklanır.

- Kastamonu Üniversitesi kurumsal kullanıcı hesabı, Kastamonu Üniversitesi kimlik kartı ve elektronik imza (token) ile yapılan tüm işlemlerden kullanıcının kendisi sorumludur.

3.10 Bilgiye Erişimin Kısıtlanması (TS ISO 27001:2013 EK A-9.4.1)

- "Erişim Kontrol Politikası" başlığı Madde 3.1'de belirtilen kurallar uygulanır.

- Kullanıcılar, kullanıcı girişi yapmadan herhangi bir uygulamaya veya bilgiye erişemez.

3.11 Güvenli Oturum Açma Prosedürleri (TS ISO 27001:2013 EK A-9.4.2)

- Sistemler ve uygulamaları yönetecek her çalışan için ayrı bir admin hesabı açılır. Varsayılan admin kullanıcı hesabı yönetimsel işlemlerde kullanılmaz.

- Oturum açma sırasında, kullanıcının bilgileri yanlış girmesi halinde, kullanıcıya hesap adı/parola yanlış vb. bilgilendirici direktifler verilir.

- Oturum açılma tamamlanmadan önce sistem/uygulama üzerindeki veriler kullanıcıya gösterilmez.

- Oturum açma sırasında kullanıcıya gerekli uyarılar mesaj/bildiri şeklinde gösterilir.

- Bu mesaj/bildiriler yetkisiz kişilere ipucu verecek bilgiler içermez.

- Oturum açıldıktan sonra bir boş kalma süresi belirlenmeli (idle time), bu sürenin sonunda oturum otomatik olarak kilit durumuna düşmelidir. Kullanıcılar tekrar hesap bilgilerini girerek oturum açabilirler.

- Kritik olarak kabul edilebilecek sistemlerde boş kalma süresi daha da kısa olacak şekilde belirlenir.

- Oturum açma kanalı şifreli kanal üzerinden yapılmalı, teknolojik çağ gereği zafiyet içeren veya zayıf kabul edilen şifreleme metotlarından kaçınılır.

- Etki Alanı (domain) kullanıcı parolasını belirlenen sayıdan fazla yanlış giren kullanıcı hesabı geçici süre kilitlenir, konu ile ilgili detaylar Bilgi İşlem Daire Başkanlığı ilgili dokümanlarında tanımlanmıştır.

- ÜBYS'de üst üste yapılan başarısız oturum açma denemeleri loglanır, konu ile ilgili detaylar Bilgi İşlem Daire Başkanlığı ilgili dokümanlarında tanımlanmıştır.

- İş bilgisayarlarında oturum açan kullanıcılara başarılı ve başarısız son oturum açma bilgisinin detayları gösterilir, konu ile ilgili detaylar Bilgi İşlem Daire Başkanlığı ilgili dokümanlarında tanımlanmıştır.

- Bilişim Sistemleri varlıklarına erişimde oturum zaman aşımı kısıtlaması uygulanır.

- Kullanıcı hesabının ihlal edildiğini veya hesabı üzerinde çok sayıda yetkisiz oturum açma denemesi yapıldığını fark ederse gerekli Olay Yönetim Politikası'na göre hareket eder.

3.12 Ayrıcalıklı Destek Programlarının Kullanımı (TS ISO 27001:2013 EK A-9.4.4)

- Kullanıcıların, sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olan ayrıcalıklı destek programlarını kullanımı mümkün olduğunca kısıtlanır,

- Destek programları uygulama yazılımlarından ayrılır,

- Madde 3.5'te belirtilen şekilde en az sayıda güvenilir ve yetkili kullanıcı sınırlandırılması uygulanır.

- Destek programları kullanım kayıtları kaydedilir.

- Destek programları kullanımı durumunda, ilgili yönetim birimi tarafından, yetkilendirme düzeyleri tanımlaması ve yazılı hale getirilmesi gerekir.

- Sistemlerde uygulama erişimi olan kullanıcıların görevden ayrılması gerektiğinde destek programlarının o kişi için kullanılamaz yapılması gerekir.

3.13. Kaynak Kodlara Erişim

- Yazılımların kaynak kodlarına Yazılım Geliştirici ve onun ilgili yöneticileri tarafından erişim sağlanır.
- Bu erişimler ve kaynak kodlar üzerinde yapılan değişiklikler loglanır.

P22 İŞ SÜREKLİLİĞİ VE FKM POLİTİKASI

1. Amaç

Bu politikanın amacı, Kurum'da gerçekleştirilen kritik faaliyetlerde iş sürekliliğinin planlanmasını, uygulanmasını, doğrulanmasını, gözden geçirilmesini ve değerlendirilmesini sağlamaktır.

2. Kapsam

Bu politika, Kurum faaliyetlerinde sadece TS ISO 27001 sertifikası bulunan birimlerdeki iş sürekliliğinin sağlanmasına yönelik hususları kapsar.

3. Politika

3.1. İş Sürekliliğinin Planlanması (TS ISO 27001:2013 Ek-A 17.1.1)

- Yönetim Birimleri, kendi faaliyetlerindeki iş sürekliliğini sağlamak amacıyla kritik faaliyetlerini İş Etki Analizi Formu (İEA) doldurarak belirlerler.

- Bilgi Güvenliği Yönetim Sistemi Ekibi, iş takip aracını kullanarak yılda bir defa tüm Yönetim Birimlerinden İş Etki Analizlerini hazırlamalarını ister.

- Bilgi Güvenliği Yönetim Sistemi Ekibi, Kurum genelinden elde edilen tüm İş Etki Analizlerinin değerlendirmesini yapar. Gerekli gördüğü noktalarda düzeltme/güncelleme talebinde bulunur.

- İş süreçlerinde, kaynaklarda yapısal, tedarikçiler veya çalışanlar düzeyindeki önemli değişikliklerde, yeni bir ürün, süreç veya teknolojiye geçişte gerçekleşen değişiklikler, kritik faaliyetlerin dolayısıyla İş Etki Analizlerinin güncellenmesini gerektirebilir. İş Etki Analizinin güncellenmesi sorumluluğu ilgili Yönetim Birimi Yöneticisine aittir.

- Bilgi Güvenliği Yönetim Sistemi Ekibi, İş Etki Analizlerinin uygulama sonuçlarından elde edilen tüm kritik faaliyetler için ilgili Yönetim Birimlerinden İş Sürekliliği Planlarını hazırlamalarını talep eder.

- Bilgi Güvenliği Yönetim Sistemi Ekibi, Kurum genelinde elde edilen tüm İş Sürekliliği Planlarının değerlendirmesini yapar. Gerekli gördüğü noktalarda düzeltme/güncelleme talebinde bulunur.

- Yönetim Birimleri ve projeler, kendi gereksinimlerini karşılayan İş Sürekliliği Planlarını oluşturulurken olumsuz durumlara yol açabilecek riskleri belirler ve takip ederler. Olumsuz durumların gerçekleşmesi halinde uygulanacak yöntemler geliştirilir, test edilir ve güncel tutulur.

- Yeni veya değişen uygulamalar, ürünler veya sistemler için iş sürekliliği planları her zaman göz önünde bulundurulur.

- İş Sürekliliği Planlarının uygulama sonuçları, Bilgi Güvenliği Yönetim Sistemi Ekibi tarafından Yönetimin Gözden Geçirilmesi toplantılarında yıllık olarak Kurum Yönetimine rapor edilir.

3.2. İş Sürekliliğinin Uygulanması (TS ISO 27001:2013 Ek-A 17.1.2)

- Kurum genelinde gerçekleştirilen kritik faaliyetler esnasında olumsuz bir olayla karşılaşılması durumunda ilgili çalışan gerekli tedbirleri alarak iş sürekliliğini sağlar ve olayı Kritik Faaliyet Sorumlusuna bildirir. Kritik Faaliyet Sorumlusu, İş Etki Analizi Formunda belirtilir.

- Kritik faaliyetlerde bir kesinti ile karşılaşılması durumunda olay Kritik Faaliyet Sorumlusuna bildirilir.

- Kritik Faaliyet Sorumlusu, bir değerlendirme yapar. Değerlendirme sonucunda olayın kritik faaliyette meydana gelen bir kesinti olduğu kararını verirse İş Sürekliliği Planını devreye sokar. Olayın kesinti olmadığı kararına varırsa gerekli gördüğü tedbirleri almak suretiyle iş sürekliliğini korumaya devam eder.

- Kesinti durumu çözüme kavuşturulduktan sonra Kritik Faaliyet Sorumlusu tarafından Bilgi Güvenliği Yönetim Sistemi Ekibine rapor edilir.

- Bilgi güvenliği ihlal olayı olarak değerlendirilen durumlar için Olay Yönetim Politikası esaslarına göre hareket edilir.

3.3. İş Sürekliliğinin Doğrulanması, Gözden Geçirilmesi ve Değerlendirilmesi (TS ISO 27001:2013 Ek-A 17.1.3)

- Yönetim Birimleri, İş Sürekliliği Planlarını ve ilgili kurtarma faaliyetlerinin geçerliliği ve etkinliğini test etmek, iş süreklilik hedefleri ile tutarlı olmasını sağlamak ve iyileştirme faaliyetlerinde bulunmak için yılda bir defa iş sürekliliği tatbikatı gerçekleştirirler. Bu tatbikatlar Bilgi Güvenliği Yönetim Sistemi Ekibi tarafından denetlenir.

- Kurumda gerçekleştirilen uygulamalar veya süreklilik bağlamında kurumsal, teknik veya süreç değişiklikleri iş sürekliliği gereksinimlerinde değişikliğe neden olabilir. İlgili Yönetim Birimi, iş sürekliliğinin sağlanması için uygulanan yöntemlerin ve kontrollerin sürekliliğini değişen koşullara karşı gözden geçirir.

3.3.1 Tatbikatların Gerçekleştirilmesi

- İş sürekliliği çalışmalarının işe yararlılığının ve eksikliklerinin tespiti için İş Sürekliliği Planının düzenli olarak tatbikatı gerçekleştirilir. Bu amaçla senelik olarak tatbikat programı hazırlanır. Tatbikat program ve formları kritik faaliyetlerin niteliğine göre değişiklik gösterebileceğinden Yönetim Birimleri kendi program ve formlarını hazırlamaktan sorumludurlar.

- İş sürekliliği yönetiminin etkin biçimde yürütüldüğünden emin olmak için gerçekleştirilecek tatbikatlara yönelik olarak izlenmesi gereken adımlar aşağıdaki tabloda verilmektedir.

Adım No	Yürüten	İşlem Adımları	Çıktılar
01	Bilgi Güvenliği Yönetim Sistemi Ekibi	Yılda bir kez, Yönetim Birimlerinden İş Sürekliliği Planı talep edilmesi	Tatbikat Planlarının Talebi
02	Yönetim Birimleri	Kurtarma planlarının doğru veriler ışığında "kritik" faaliyetler için oluşturulması	Tatbikat Takvimi
03	Yönetim Birimleri	İş Sürekliliği Tatbikatından etkilenecek kişi/grupların haberdar edilmesi	Tatbikat Bildirimi
04	Yönetim Birimleri	İş Sürekliliği Tatbikatının gerçekleştirilmesi	Gerçekleşmiş Tatbikat
05	Yönetim Birimleri	İş Sürekliliği Tatbikat Formunun hazırlanması ve Bilgi Güvenliği Yönetimi Birimi'ne gönderilmesi	Tatbikat Formu
06	Bilgi Güvenliği Yönetim Sistemi Ekibi	İş Sürekliliği Tatbikat Formlarının değerlendirilmesi ve önceki tatbikatların sonuçları ile kıyaslanması	Tatbikat Kıyaslaması
07	Bilgi Güvenliği Yönetim Sistemi Ekibi	Sonuçların iş sürekliliği ile ilgili iyileştirmeler için kullanılması	İyileştirmeler
08	Bilgi Güvenliği Yönetim Sistemi Ekibi	Elde edilen sonuçların yıllık yapılan Yönetimin Gözden Geçirme (YGG) toplantılarında sunulması	YGG Toplantı Tutanağı

3.4 Bilgi İşleme Olanaklarının Erişilebilirliği (TS ISO 27001:2013 Ek-A 17.2.1)

- Yedek Fazlalıklar Kurum'un Yedekleme Prosedürü baz alarak yapılmaktadır.

P23 LOG YÖNETİMİ POLİTİKASI

1. Amaç

Bu politika, Kurum'un uymakla yükümlü olduğu mevzuat gereği sistemler üzerinde gerçekleşen olayların toplanması, yönetilmesi ve kaydedilmesi, sistem kullanımları incelenerek kullanıcıların rol ve sorumlulukları gereğince sahip oldukları erişim yetkileri doğrultusunda yapmış oldukları eylemlerin izlenmesi amacıyla hazırlanmıştır.

2. Kapsam

Bu politika, Kurum'a bağlı Yönetim Birimleri, bilişim sistemleri, iş süreçlerinde kaydedilen loglarla ilgili kayıt ve izleme faaliyetlerini kapsamaktadır.

3. Politika

3.1 Olay Kaydetme (TS ISO 27001:2013 Ek-A.12.4.1)

- Loglar; güvenlik yazılımları (antivirüs, güvenlik duvarı, saldırı tespit ve saldırı önleme gibi), sunucu işletim sistemleri, ağ cihazları ve uygulama yazılımları gibi pek çok kaynak tarafından üretilmektedir.
- Log yönetimi altyapısı, sistemlerin ve ağ performansının en uygun hale getirilmesi, kullanıcı hareketlerinin kaydedilmesi, zararlı aktivitelerin belirlenmesi için gerekli verilerin sağlanması ve güvenlik olaylarının soruşturulması gibi amaçlarla log verisinin üretimi, konsolidasyonu, analizi ve güvenliğini destekleyen işlevleri gerçekleştirir.
- TS ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi kapsamında logların kaydedilmesi, korunması, saklanması ve düzenli olarak gözden geçirilmesi için gereken faaliyetler Log Yönetim Sorumluları tarafından yürütülmelidir.
- İlgili kayıtlar, mümkün olduğunca merkezi log sunucusu veya ilgili uygulamalar üzerinde tutulmaktadır. Bu kapsamda aşağıda belirtilen kayıtlar alınmaktadır;
  - KBTS'ye dahil edilmiş bilgisayarlardaki kullanıcı kimlikleri,
  - Oturum açma ve oturum kapatma gibi anahtar olayların tarihleri, saatleri ve detayları,
  - Cihaz kimliği,
  - Başarılı ve reddedilmiş sistem erişim girişimlerinin kayıtları,
  - Başarılı ve reddedilmiş veri ve diğer kaynaklara erişim girişimlerinin kayıtları,
  - Sistem araçları ve uygulamalarının kullanımı,
  - Erişilen dosyalar ve erişim türü,
  - Ağ adresi ve protokolleri,

3.2 Bilgi Sistemleri Kayıtları

- Kurum Bilgi Sistemleri bünyesinde uygulama ajanı veya syslog servisi ile sistemler üzerinde oluşan bütün olaylar, mümkün olduğu sürece log yönetim yazılımında Log Yönetim Sorumluları tarafından toplanmalı ve analiz edilmelidir.
- Sistemlerden toplanması beklenen olay kayıtları aşağıda verilmektedir;
  - Sunucu ve KBTS'ye dahil kullanıcı bilgisayarlarında;
    - ❖ Sisteme giriş ve çıkış kayıtları
    - ❖ Yetkisiz erişim denemeleri
  - Ağ güvenlik cihazları üzerinde;
    - ❖ Erişilen kaynak ve hedef sistemler
    - ❖ Erişilen kaynak ve hedef portlar
    - ❖ Erişim zamanları
  - Saldırı Tespit Sistemi ve antivirüs sunucusu üzerinde;
    - ❖ Sistemlerde tespit edilen zararlı yazılımlar
    - ❖ Sistemlere yapılan saldırılar ve normal olmayan erişim istekleri

3.3 Fiziksel Erişim Logları

- Kameralar, kurum yerleşkesinin fiziki sınırlarında kayıt yapmaktadır. Ayrıca sistem odasının iç ve dış giriş çıkış kontrolü için kameralar bulunmaktadır. İdari ve Mali İşler Daire Başkanlığına bağlı Güvenlik Amirliği tarafından görüntüler takip edilmektedir. Bu kayıtlar en az yirmi gün saklanmaktadır.
- Kapı giriş kontrol sistemi tüm giriş ve çıkış olaylarının loglarını üretir. Loglar, kapı giriş kontrol sisteminin üzerinde çalıştığı cihaz/sunucuda tutulur. Cihaz/Sunucu üzerinde son 5 yıla ait loglar bulunur.

3.4 Kayıt Bilgisinin Korunması (TS ISO 27001:2013 Ek-A.12.4.2)

- Üretilen bütün log kayıtları, öncelikli olarak kaydı üreten cihaz üzerinde depolanır.
- İş Sürekliliği Etki Analizi sonucu etkisi "Çok Yüksek" olarak belirlenen sistemler ve Bölüm tarafından log kaydı tutulması talep edilen uygulamaların kayıtları merkezi log sunucusuna öncelikli olarak aktarılır (İş Sürekliliği ve FKM Politikası). Diğer uygulamaların logları kendi sunucuları üzerinde tutulur.
- Kayıtlara sadece Log Yönetim Sorumluları tarafından erişilir.
- Kayıt analiz yazılımı kullanıldığında yazılım orijinal kayıtlara zarar vermez.

- Kayıtlar mevzuat gereği belirtilen süre kadar saklanır.
- Gerekli logların sağlıklı/eksiksiz bir şekilde tutulup tutulmadığı senede en az bir kere kontrol edilir.
- Kayıtların bulunduğu ortamların imhası Kabul Edilebilir Kullanım Politikası'na ve Kastamonu Üniversitesi Kişisel Veri Saklama ve İmha Politikası'na göre gerçekleştirilir.
- Log kayıtlarını barındıran log sunucusu, Yedekleme Prosedürüne uygun olarak yedeklenir.
- Arşivlenen logların veri saklama dönemi sonuna gelindiğinde uygun şekilde silinmesi ve imha edilmesinin koordinasyonundan Log Yönetim Sorumluları sorumludur.

3.5 Yönetici ve Operatör Kayıtları (TS ISO 27001:2013 Ek-A.12.4.3)

- Log yönetim sistemindeki loglar iş gereksinimlerine bağlı olarak Sistem Yöneticileri, Uygulama Yöneticileri, Ağ Yöneticileri ve Bilgi İşlem Daire Başkanı'na okuma erişim hakkı ile verilebilir.
- Log kayıtları gizlilik, bütünlük ve erişilebilirlik ihlallerine karşı korunur. Log kayıtlarına, ilgili sistemin yönetiminden sorumlu personel haricinde, hiçbir personele okuma, yazma veya değişiklik amaçlı erişim izni verilmez.

3.6 Saat Senkronizasyonu (TS ISO 27001:2013 Ek-A.12.4.4)

- Log kaynağına ait sistem zamanının tutarsız veya anlamsız olmaması için log kaynaklarına ilişkin zaman bilgisi tekil bir NTP sunucusu ile uyumlu hale getirilir.
- Log yönetimi sistemine loglar mümkün olduğu kadar gerçek zamanlı olarak aktarılır. İlgili sistemin gerçek zamanlı aktarımı desteklememesi durumunda belirli bir zamanda çalıştırılan otomatik görev (task) ile aktarılır.
- Saat senkronizasyonu bütün sistemleri kapsayacak şekilde yapılır.

P24 SANALLAŞTIRMA POLİTİKASI

1. Amaç

Bu politika, Kurum bünyesinde kullanılan sanal makinelerde uyulması gereken güvenlik prensiplerini düzenlemek amacıyla hazırlanmıştır.

2. Kapsam

Bu politika Kurum bünyesinde kullanılan sanal makineleri kapsamaktadır.

3. Politika

3.1. Hipervizör Güvenliği

Hipervizör güvenliği ile ilgili aşağıdaki tabloda yer alan gereksinimler uygulanır:

Yama Yönetimi	Hipervizör üzerinde üretici firma tarafından yayımlanan tüm yamalar yüklenir.
Erişim Kısıtlama	Hipervizörün yönetim ara yüzüne erişim kısıtlanır.
İletişimin Şifrelenmesi	Hipervizörün bulunduğu yönetim ağı haberleşmesi şifrelenir.
Varlık Yönetimi	Sanal makineler, Varlıkların Kabul Edilebilir Kullanım Politikası'na göre oluşturulur ve yönetilir.
Konfigürasyon Yönetimi	Hipervizörün konfigürasyon yönetimi merkezi olarak yapılır ve tüm konfigürasyonlar dokümante edilir.
Senkronizasyon	Sanallaştırma altyapısı, Kurum bünyesinde kullanılan zaman sunucusuyla senkronize edilir.
Kullanılmayan Donanım	Host sistemlerden kullanılmayan donanımların bağlantısı kesilir.
Gereksiz Servisler	Hipervizör üzerinde gereksiz olan servisler kapatılır.
İzleme	Hipervizör üzerindeki olaylar kayıt altına alınır ve izlenir.
Üretim ve Test Ortamı	Sanal makineler, üretim ve test ortamlarında bulundurulur.

3.2. Konuk İşletim Sistemi Güvenliği

Konuk (guest) işletim sistemi güvenliği ile ilgili aşağıdaki tabloda yer alan gereksinimler uygulanır**:**

Uygulanacak Politikalar	Log Yönetimi Politikası ve Uzaktan Çalışma Politikası dokümanlarında yazan hususlar uygulanır.
Konfigürasyon Yönetimi	Konuk işletim sistemlerinin konfigürasyon yönetimi merkezi olarak yapılır.
Yama Yönetimi	Zafiyet ve Yama Yönetimi Politikası'na uygun şekilde yama yönetimi gerçekleştirilir.

Yedekler	Düzenli olarak konuk işletim sistemlerinin yedeği alınır ve yedekten geri dönüş testleri uygulanır.
Kullanılmayan Donanım	Konuk bilgisayarlarda kullanılmayan donanımların bağlantısı kesilir.
Kimlik Doğrulama	Her bir konuk bilgisayar için yerel kimlik doğrulama mekanizmaları kullanılır.
Zafiyet Yönetimi	Konuk bilgisayarlar üzerinde yapılacak açıklıkların tespitinde Zafiyet ve Yama Yönetimi Politikası'nda yer alan hususlar dikkate alınır.
İletişimin İzlenmesi	Konuk bilgisayarlar arasındaki haberleşme kayıt altına alınır.

P25 SOSYAL MEDYA KULLANIM POLİTİKASI

1. Amaç

Bu politika, Kurum personelinin sosyal medya kullanımı prensiplerini düzenlemek amacıyla hazırlanmıştır.

2. Kapsam

Bu politika Kurum'a bağlı birimlerde çalışan personelin, öğrencilerin ve hizmet alımı ile çalışan personelin sosyal medya kullanımını kapsamaktadır.

3. Politika

- Kurum seviyesinde bilgi güvenliğinin sağlanabilmesi için tüm çalışanların bilgi güvenliği sorumlulukları bulunmaktadır. Bilgi Güvenliği sağlanırken insan faktörünün payı teknik önlemlerden çok daha büyüktür. Güvenlik seviyesini belirlemek için en zayıf halkaya bakılmaktadır. Bilgi güvenliğinde en zayıf halka insandır.
- Teknik olarak ne kadar önlem alınırsa alınsın, bilgi güvenliği farkındalığının düşük olduğu kullanıcıların bulunduğu bir ortamda güvenliği sağlamak mümkün değildir.
- İnsan faktörünü kullanan saldırı tekniklerinden ya da kişiyi etkileme ve ikna yöntemlerinden faydalanarak normal koşullarda kişilerin gizlemeleri / paylaşmamaları gereken bilgileri bir şekilde ele geçirme sanatı Sosyal Mühendislik olarak ifade edilmektedir.
- Kuruma ait gizli kalması gereken bilgileri, veri aktarımı vb. maksatlarla geçici süre için olsa bile Kurum kontrolünde olmayan depolama alanlarında (Google Drive, iCloud, Yandex Disk, We Transfer, Rapid Share vb.) saklanmamalıdır. Mobil uygulamalar (WhatsApp, Massenger, Line, Viber, Telegram, WeChat, Skype, SnapChat vb.) ve sosyal medya platformları (Facebook, Youtube, Instagram, Twitter, Linkedin vb.) üzerinde işletilmemelidir. Şahsi e-posta hesapları (*@gmail.com, *@yandex.com vb.) üzerinden aktarılmamalıdır.
- Sosyal medya hesaplarında kullanılan parolalar ile Kurum içinde kullanılan parolalar farklı olmalıdır.
- Kullanılan parolanın güçlü olabilmesi için aşağıdaki maddeleri sağlıyor olması gerekmektedir.
  - En az sekiz karakter uzunluğunda olmalıdır. (********)
  - Büyük harf, küçük harf, en az bir rakam ile en az bir özel karakter içermelidir.
  - Sıralı harf veya rakamlardan oluşmamalıdır.

- Kolayca erişilebilen veya tahmin edilebilecek doğum tarihi, telefon numarası gibi kişisel bilgiler içermemelidir.
- Herhangi bir dilin sözlüğünde bulunan kelimeler, özel isimler ve tersten yazılmış haller kullanılmamalıdır.
- Kolay hatırlamak amacıyla açık bir şekilde yazılı olarak parolalar bulundurulmamalıdır.
- Kastamonu Üniversitesi resmi sosyal medya hesapları dışında üçüncü kişiler tarafından paylaşılan hiçbir içerikten sorumlu değildir.
- Kurum bünyesinde çalışan personel, öğrenci ve hizmet alımı ile çalışan personel kuruma ait ve gizlilik ve kritiklik değeri olan herhangi bir raporu/belgeyi/veriyi Resmi ve Diğer Sosyal medyada paylaşmamalıdır.
- Kurum bünyesinde çalışan personel, öğrenci ve hizmet alımı ile çalışan personel kurum bünyesinde yapılan kritik ve gizlilik değeri olan işler hakkında Resmi ve Diğer Sosyal medyada paylaşım yapmamalıdır.
- Resmi ve Diğer Sosyal Medya hesaplarında, yayımlanması gereken, isim listesi, sınav sonuç listesi vb. kişisel veri içeren dokümanları paylaşırken KVKK gereğince, veriler maskelenmelidir.
- Resmi ve Diğer Sosyal Medya hesaplarında fotoğraf ve videolarda yer alan çalışanlarımızın/öğrencilerimizin görüntüleri ancak izinleri alınmışsa yayımlanabilir, bunun dışında hizmet verdiğimiz birimlerin, tedarikçilerimizin, ziyaretçilerimizin görüntülerine, izinleri alınmadığı takdirde yer verilmemeli, paylaşımlarda, adları etiketlenmemelidir.
- Resmi Sosyal Medya hesaplarında, hiçbir ticari ürünün/hizmetin reklamı, hiçbir siyasi görüşün propagandası yapılmamalı; herhangi bir kişi ve/veya kurumu, hizmeti, ürünü kötüleyen, küçük düşüren yorumlar yapılmamalıdır.
- Kastamonu Üniversitesi, resmi sosyal medya hesaplarında gelen yorum, mesaj ve gönderilere izin vermeme, silme, gizleme ve yayımlayan kullanıcıyı yasaklama/engelleme hakkını saklı tutar

P26 TEDARİKÇİ İLİŞKİLERİ BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bu Politikanın amacı, Kurum ile tedarikçiler arasında yapılan anlaşmalarla uyumlu seviyede bilgi güvenliği ile hizmet tedarikinin sürekliliğini ve tedarikçiler tarafından erişilebilen Kurum'a ait bilgi varlıklarının korunmasını sağlamaktır.

2. Kapsam

Bu politika, Kurum ile tedarikçiler arasında yürütülen işlemlerde bilgi güvenliğinin sağlanmasına yönelik hususları kapsar.

Politika

3.1 Tedarikçi İlişkileri İçin Bilgi Güvenliği Politikası (TS ISO 27001:2013 Ek-A 15.1.1)

- Kurum, gerçekleştirdiği faaliyetlerin niteliğine bağlı olarak kendi bilgisine erişim izni verdiği tedarikçileri ile Gizlilik Sözleşmesi imzalamak suretiyle bilgi güvenliği kontrolleri yapmayı ve bu kontrollere uymaları için tedarikçilerine gerekli yönlendirmelerde bulunmayı Bu Politikaya göre uygular.
  - Kurum'un bilgilerine erişim izni verilen tedarikçilerin faaliyet alanlarına göre türleri Satın alma Yönetimi Süreç Tanımlama Dokümanı altındaki Tedarikçi Listesi'nde verilir.
  - Kurum, tedarikçi ilişkilerini Satın alma Prosesi Dokümanına göre yönetir.
  - Kurum, tedarikçilerinin farklı türleri için tanımlanan bilgi erişimlerine izin verilmesi, erişimlerin izlenmesi ve kontrol edilmesi faaliyetlerini tedarikçisi ile arasında imzaladığı Gizlilik Sözleşmesi'ne göre yürütür.
  - Birim satın alma iş ve işlemlerinden sorumlu personel, satın alma talebinde belirlenen ihtiyacı inceleyerek tedarikçinin Kurum bilgisine erişim sağlayıp sağlamaması gerekliliği durumunu değerlendirir. Gerekli görürse talep sahibi ile iletişime geçer. Erişim sağlanması gerekiyorsa satın alma işleminden sorumlu personel, Kurum ihtiyaçlarını ve tedarikçinin risk profilini temel alarak bilgi ve erişim türüne göre bilgi güvenliği gereksinimlerini belirler, Gizlilik Sözleşmesi taslağını hazırlar.
  - Kurum bilgisi, yetersiz bilgi güvenliği yönetimi nedeniyle tedarikçi tarafından riske atılabilir. Bu riski ortadan kaldırmak için tedarikçinin Kurum bilgisine erişiminin yönetilmesi; doğruluk ve bütünlüğe ilişkin gerekli kontrollerin tespit edilmesi ve uygulanması işlemleri Gizlilik Sözleşmesi'ne göre gerçekleştirilir.

- Kurum bilgisini korumak için tedarikçilere uygulanan yükümlülükler Gizlilik Sözleşmesi'nde belirtilir.
- İhtiyaç olması durumunda Kurum ve tedarikçi arasında paylaşılan bilgi ve bilgi işleme kullanılabilirliğini yeniden sağlamak için gerekli kurtarma ve acil durum düzenlemeleri Gizlilik Sözleşmesi'nde belirtilir.
- Kurumun ve tedarikçilerinin sorumlulukları dâhil olmak üzere tedarikçi erişimi ile ilişkili acil durumlar ve ihlal olayları Olay Yönetim Politikası'na göre yönetilir.
- Taraflarca, bilgi güvenliği şartları ve kontrollerinin yazılı olduğu bir anlaşmanın hangi şartlar altında imzalanacağı taslak sözleşmede belirtilir.
- Birim satın alma iş ve işlemlerinden sorumlu personel, Kurum ihtiyaçlarını ve tedarikçinin risk seviyesini temel alarak bilgi ve erişim türüne göre bilgi güvenliği gereksinimlerini belirler, Gizlilik Sözleşmesi taslağını hazırlar.
- Birim satın alma iş ve işlemlerinden sorumlu personel, Gizlilik Sözleşmesi taslağını kontrol etmek üzere Birim Gerçekleştirme Görevlisi ve Harcama Yetkilisine gönderir.
- Birim Harcama Yetkilisi ve Gerçekleştirme Görevlisi, oluşturulan taslak sözleşmeyi inceleyerek düzeltme ihtiyacı olup olmadığına karar verir. Düzeltme ihtiyacı olan yerleri Birim satın alma iş ve işlemlerinden sorumlu personel bildirir. Düzeltme ihtiyacı olmadığı durumlarda taslağı onaylar. Gerekli durumlarda taslak sözleşme üzerinde görüş almak üzere Üniversitemiz Hukuk Müşavirliğinden görüş talebinde bulunur.
- Birim satın alma iş ve işlemlerinden sorumlu personel, Sözleşme Taslağını tedarikçiye göndererek mutabakat sağlamak (doğruluk ve bütünlük kontrolleri) üzere görüşmeye başlar. Taslak üzerinde değişiklik yapılması gereken durumlarda gerekli güncellemeler yapılarak, Birim Harcama Yetkilisi veya Gerçekleştirme Görevlisinin onayına sunulur.
- Birim satın alma iş ve işlemlerinden sorumlu personel, tedarikçi gözden geçirme ve ürün doğrulama dâhil her tedarikçi türü ve erişim türü için kurulan bilgi güvenliği gereksinimlerinin uyumluluğunu izler.
- Bilgi Güvenliği Yönetim Sistemi Ekibi, uygulanabilir politikalar, süreçler, tedarikçilerin Kurum sistemleri ve bilgilerine erişim düzeyleri ve tedarikçi türlerine göre uygun katılım ve davranış kuralları konusunda Satın Alma Birimi çalışanlarına farkındalık eğitimi verir.
- İhtiyaç olması durumunda Kurum ve tedarikçi arasında paylaşılan bilginin paylaşılması, bilgi işleme tesislerinin veya her türlü varlığın taşınması işlemleri sırasında bilgi güvenliğinin sağlanması, Gizlilik Sözleşmesi'ne göre yürütülür.

3.2 Tedarikçi Anlaşmalarında Güvenliği İfade Etme (TS ISO 27001:2013 Ek-A 15.1.2)

- Kurum bilgisine erişebilen, bunu işletebilen, depolayabilen, iletebilen tedarikçiler ile belirlenen tüm bilgi güvenliği gereksinimleri Gizlilik Sözleşmesi ile belirlenir. Gizlilik Sözleşmesi'nde aşağıdaki hususlar dikkate alınır:
  - Tedarikçinin erişeceği bilginin tanımı ve erişim yöntemleri belirtilir.
  - Varlıkların Kabul Edilebilir Kullanım Politikası'na uygun olarak bilgi sınıflandırılır (bilginin yasal gereksinimleri, değeri, kritikliği ve yetkisiz ifşa veya değiştirilmeye karşı hassasiyetine göre sınıflandırılması), gerekli görülürse Kurum'un kendi sınıflandırma düzeni ile tedarikçi sınıflandırma düzeni arasında eşleştirme yapılır.
  - Kurum verilerinin korunması, fikri mülkiyet hakları ve telif hakları dâhil yasal ve düzenleyici gereksinimler ve bunların nasıl karşılanacağı açıklanır.
  - Erişim kontrolü, performans gözden geçirme, izleme, raporlama ve denetimi içeren üzerinde anlaşılmış kontrol maddelerini uygulamak için her iki tarafın yükümlülükleri belirtilir.
  - Bilginin kullanımına ilişkin kurallar açıklanır.
  - Kurum'un bilgisine erişmek veya almak için yetkilendirilecek tedarikçi çalışanının açık listesi, yetkilendirme ve yetkilendirmenin kaldırılması için gerekli şartlar belirtilir.
  - İhlal olayı yönetimi gereksinimleri ve süreçleri, özellikle ihlal olayına müdahale esasında bildirim ve ortak çalışma hususları açıklanır.
  - Sözleşmeye yönelik bilgi güvenliği politikaları belirtilir.
  - Belirli süreçler ve bilgi güvenliği gereksinimleri için eğitim ve farkındalık gereksinimleri belirtilir (örneğin; ihlal olayına müdahale, yetkilendirme süreçleri vb.).
  - Sözleşmeye, bilgi güvenliği konularında irtibat kişisi de dâhil olmak üzere anlaşmanın tarafları yazılır.
  - Gerekli görülmesi durumunda tedarikçi firma çalışanı geçmiş taramasının tamamlanmadığı veya sonuçların şüphe veya çekinceye neden olduğu durumlarda taramanın gerçekleştirme ve bildirim süreçleri için sorumluluklar da dâhil olmak üzere tedarikçi firma çalışanı için tarama gereksinimleri oluşturulur.
  - Kurum'un tedarikçi firmanın anlaşmaya yönelik süreçlerini denetleme hakkının olduğu belirtilir.
  - Sorunların ve anlaşmazlıkların çözümü ile ilgili hukuki süreçler belirtilir.

- Periyodik kontrollerin etkinliği konusunda bir rapor oluşturulması için tedarikçinin yükümlülüğü ve raporda gündeme getirilen hususların zamanında düzeltilmesi konusunda anlaşma sağlanır.
- Kurum'un güvenlik gereksinimleri ile uyumluluk için tedarikçi yükümlülükleri belirtilir.

3.3 Bilgi ve İletişim Teknolojileri Tedarik Zinciri (TS ISO 27001:2013 Ek-A 15.1.3)

- Tedarik zinciri güvenliğini sağlamak için tedarikçilerle yapılan anlaşmalarda aşağıdaki hususlar dikkate alınır:
  - Tedarikçi ilişkileri için genel bilgi güvenliği şartlarını içeren Gizlilik Sözleşmesi'ne ek olarak bilgi ve iletişim teknolojileri ürün veya hizmet temininde uygulanmak üzere bilgi güvenliği şartları tanımlanır.
  - Kurum ile tedarikçiler arasında tedarik zinciri, diğer olası konularda ve uzlaşılarda bilgi paylaşımı için gerekli kurallar Satın alma irimi tarafından belirlenir.
  - Sadece bilgi ve iletişim teknolojisi hizmetleri satın alımı sürecine özgü olarak şayet tedarikçiler Kurum'a sağlanan ürünlerin tamamında veya bir bölümünde diğer tedarikçilerden alım yapıyorsa tedarik zinciri boyunca Kurum'un güvenlik gereksinimlerinin yaygınlaştırılması birim satın alma iş ve işlemlerinden sorumlu personel tarafından sağlanır.
  - Tedarikçiden teslim alınan bilgi ve iletişim teknolojisi ürünlerinin teknik şartnamede ve sözleşmede belirtilen tüm özellikleri sağladığının tespitinden ve onay/reddinden Muayene ve Kabul Komisyonu sorumludur.
  - Yükleniciler ile yapılan sözleşmelerde, tedarik edilen bilgi ve iletişim teknolojileri ürün ve hizmetleri için tedarik zinciri ile ilişkili riskler göz önünde bulundurulmalı ve ilgili güvenlik gereksinimlerinin sözleşme içeriklerine eklenmesinden ve bu kapsamda, birlikte çalışılacak kişi ve/veya kuruluşlardan tedarik zinciri güvenliğinin temin edileceğine dair yazılı belge alınmasından Harcama Yetkisi/ Gerçekleştirme Görevlisi/ Birim Satın Alma İş ve İşlemlerinden Sorumlu Personel sorumludur.
  - Kurum ile tedarikçiler arasında tedarik zinciri boyunca bilgi paylaşımı kuralları tanımlanır.
  - Kurum için kritik bileşenlerin ve bunların kaynaklarının ediniminin takip edilebilirliği Birim Satın Alma İş ve İşlemlerinden Sorumlu Personel tarafından güvence altına alınır.

3.4 Tedarikçi Hizmetlerini İzleme ve Gözden Geçirme (TS ISO 27001:2013 Ek-A 15.2.1)

- Kurum ile tedarikçileri arasındaki hizmet yönetimi ilişkisinden satın alma talebinde bulunan ve teslim edilen ürünün işletilmesinden yetkili personel sorumludur ve tedarikçiler tarafından

Kurum'a sağlanan hizmetlerin izlenmesi, gözden geçirilmesi, bilgi güvenliği şart ve koşullarına riayet edildiğini aşağıdaki hususları dikkate alarak yönetir:

- Tedarikçilerle yapılan anlaşmalara riayet edildiğini kontrol etmek için tedarikçilerin hizmet performansı düzeylerini izler.
- Anlaşmalarda belirtilmesi durumunda tedarikçiler tarafından üretilen hizmet raporlarını gözden geçirir ve gerekli görürse ilerleme toplantıları düzenler.
- İç/dış denetim raporlarında belirtilen bulgular olması durumunda bunları dikkate alarak tedarikçileri denetler ve tespit edilen hususları takip ederek düzeltilmesini sağlar.
- Hizmetlerin teslimatı ile ilgili olası kesintileri ve hataları izler, işletim sorunları, hatalar ve bilgi güvenliği olayları kayıtları ve tedarikçi denetim kayıtlarını gözden geçirir.
- Herhangi bir problem veya ihlal olayı tespit edilmesi durumunda çözülmesi faaliyetlerini başlatır.
- Yaşanabilecek büyük hizmet kesintileri ve felaketlerden sonra tedarikçinin yeterli hizmet yeteneğinin devamlılığının sağladığından emin olunmasını sağlar.
- Tedarikçinin anlaşma gereksinimlerine uymasını sağlamak ve uygulanmasını gözden geçirmek için tedarikçinin kendi organizasyonu içerisinde gerekli sorumlulukları atadığını denetler.
- Tedarikçilerin (varsa) kendi tedarikçileri ile ilişkilerinin bilgi güvenliği yönünden gözden geçirilmesini sağlar.
- Tedarikçi tarafından erişilen, işlenen ve yönetilen hassas ve kritik bilgilerin yeterli derecede genel kontrolünü ve görünürlüğünün sürdürülmesini sağlar.
- Hizmetin teslimatında eksiklikler tespit edilmesi durumunda uygun eylemleri gerçekleştirir.
- Bilgi güvenliği ihlal olayları hakkında bilgi sağlanması ve anlaşmalar, tüm destekleyici kılavuzlar ve süreçler gereği bu bilgilerin gözden geçirilmesi için Olay Yönetim Politikası dokümanına göre hareket eder.

3.5 Tedarikçi Hizmetlerindeki Değişiklikleri Yönetme (TS ISO 27001:2013 Ek-A 15.2.2)

- Birim Satın Alma İş ve İşlemlerinden Sorumlu Personel, tedarikçilerin hizmet tedarik yöntemlerinde değişikliğe gitmeleri durumunda, Kurum'un mevcut bilgi güvenliği politikalarının, süreçlerinin ve kontrollerinin sürdürülmesini ve iyileştirmesini kapsayacak şekilde iş bilgisi, sistem ve süreçlerin kritikliğini ve risklerin yeniden değerlendirmesini hesaba katarak süreci yönetir. Bu süreç yönetilirken aşağıdaki hususları dikkate alır:

- Tedarikçi anlaşmalarındaki olası değişiklikler takip edilir.

- Kurum tarafından yapılan aşağıdaki değişiklikler dikkate alınır:
  - Mevcut hizmetlerin zenginleştirilmesi,
  - Yeni uygulamaların ve sistemlerin geliştirilmesi,
  - Politika ve süreçlerdeki olası değişiklikler ve güncellemeler,
  - Bilgi güvenliği olaylarını çözmek ve güvenliği artırmak için yeni kontroller.
- Tedarikçi tarafından yapılan aşağıdaki değişiklikler izlenir:
  - Tedarikçi ağlarının değişimi ve genişletilmesi,
  - Yeni teknolojilerin kullanımı,
  - Yeni ürün veya yeni sürümlerin adapte edilmesi,
  - Yeni geliştirme araçları ve ortamları,
  - Hizmet tesislerinin fiziksel konumlarının değişimi,
  - Tedarikçilerin değişimi,
  - Başka bir tedarikçi kullanılması durumu.

P27 UZAKTAN ÇALIŞMA POLİTİKASI

1. Amaç

Bu Politika, Kurum personelinin uzaktan çalışma prensiplerini düzenlemek amacıyla hazırlanmıştır.

2. Kapsam

Bu Politika Kurum'a bağlı Yönetim Birimlerinde çalışan personel ve hizmet alımı ile çalışan personelin uzaktan çalışma kural ve koşullarını kapsamaktadır.

3. Politika

3.1 UZAKTAN ERİŞİM KURALLARI

- Farklı bir fiziksel lokasyondan Kurum ağı ve sistemlerine erişim için VPN (Sanal Özel Ağ) kullanılmalıdır.
- Kurum ağına VPN ile bağlanılması gerektiğinde, ÜBYS Destek Modülünden talep açılması gerekmektedir. Çalışanlar Uzak Bağlantı Talep Formunu doldurarak kullanım kurallarını okuduğunu ve uymayı kabul ettiğini taahhüt etmektedir. Formda, erişmek istenilen kaynak ve servis bilgileri belirtilmelidir. Uzaktan erişim talepleri, Bilgi İşlem Daire Başkanlığı Yönetici Islak İmzalı Onayı ile yerine getirilmektedir.
- Kurum sistemlerine uzaktan erişim aktiviteleri kayıt altına alınmaktadır.

3.2 UZAKTAN ÇALIŞMA KOŞULLARI

- Uzaktan bağlantı (VPN) izni verilen yönetim birimlerinde; bağlantı yapılacak ağın güvenliğinden emin olunması gerekmektedir.
- Halka açık olan ağlardan kurumsal iş bilgisayarları ile kablolu/kablosuz bağlantı kurulmamalıdır ve VPN bağlantısı yapılmamalıdır. Kurum ağına uzaktan bağlantı sırasında bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerlerinin korunması bağlantıyı gerçekleştiren çalışanın sorumluluğundadır.
- Uzaktan erişim yetkisi tanımlanan çalışan, yetkilerini diğer Kurum çalışanları veya üçüncü taraf kişilere kullandırmamalıdır.
- Bağlantı yapan cihazda kuruma ait güncel anti-virüs yazılımı kurulumu olmadır.
- VPN oturumundan sorumlu olan çalışan; yaptığı VPN bağlantısının ifşa olması, hesabının ele geçirilmesi, hali hazırda var olan zararlı yazılımın kasıtlı / kasıtsız Kurum ağına bulaşması ile ilgili dikkatli davranmalıdır.

P28 VERİ ENVANTERİ POLİTİKASI

1. Amaç

Bu Politika, Kurum bünyesinde kullanılan bilgi/belge/dokümanlar için veri sınıflandırmasıyla ilgili güvenlik prensiplerini içermektedir.

2. Kapsam

Bu politika Kurum bünyesinde kullanılan bilgi/belge/dokümanları kapsamaktadır.

3. Politika

- Bilgi varlıkları "TASNİF DIŞI", "HİZMETE ÖZEL", "ÖZEL". GİZLİ" VE "ÇOK GİZLİ" etiketlerinden birine sahip olmalıdır.
- Kurum içerisinde "ÇOK GİZLİ" gizlilik derecesinden daha üst düzeyde bilgi/belge/doküman işlenemez.
- "ÖZEL". GİZLİ" VE "ÇOK GİZLİ" gizliliğe sahip kurumsal bilgiler; kastamonu.edu.tr uzantılı e-posta sisteminde ve EBYS'de oluşturulamaz/bulundurulamaz.
- Bilgi varlıklarına erişim yetkileri Erişim Kontrol Politikası'na uygun olarak varlığın gizlilik derecesi dikkate alınarak verilir.
- Bilginin kalıcı ya da geçici kopyaları, bilginin orijinaline uygulanan koruma önlemlerine uygun olarak korunur.
- HİZMETE ÖZEL ve üstü gizlilik dereceli bilgi içeren taşınabilir donanımlar Kurum dışına çıkartılacaklarında, bilginin gizlilik seviyesine uygun olarak şifreleme yapıldığından emin olunmalıdır.
- İnternet üzerinden "ÖZEL", GİZLİ" VE "ÇOK GİZLİ" gizlilik dereceli bilgiler paylaşılmaz.

P29 ZAFİYET VE YAMA YÖNETİMİ POLİTİKASI

1. Amaç

Bu Politika, Kurum'daki bilgi sistemlerinde yaşanabilecek teknik açıklıkların yönetimini ve tetkik kontrolleri ile ilgili hususları belirtmek amacıyla yazılmıştır.

2. Kapsam

Bu Politika Kurum Bilgi Güvenliği Yönetim Sistemi kapsamına giren sistemlerde yaşanabilecek teknik açıklıklarla ilgili yürütülen faaliyetleri kapsamaktadır.

3. Politika

3.1. Teknik Açıklıkların Yönetimi (TS ISO 27001 EK A-12.6.1)

3.1.1 Teknik Açıklık Taramalarının Planlanması

- Teknik açıklıkları belirlemek için kullanılacak bilgi kaynakları; varlık envanter listesinde bulunan tüm yazılım ve donanımlar kullanılarak tanımlanmalıdır.
- Teknik açıklık taramalarının sıklığı, sistemin ilişkili olduğu verinin kritikliğine göre, varlığın sahibi ve Bilgi İşlem Daire Başkanlığı tarafından belirlenir. BGYS Proje Sorumlusu bilgilendirilir.
- Kurum genelindeki izleme, yama, varlık izleme ve teknik açıklık yönetimi BGYS Proje Sorumlusu koordinasyonunda gerçekleştirilir.
- Genel sistem taramaları için BGYS iç denetiminden önce açıklık tarama planlaması yapılır ve uygulamaya alınır.
- Tarama kapsamında incelenecek sistemler, Bilgi İşlem Daire Başkanlığı tarafından IP adres aralığı, web uygulamaları, kritik sunucular ve diğer parametreler göz önünde bulundurularak belirlenir. Kritik olarak belirlenen sistemler öncelikli olarak tanımlanmalıdır.
- Kurum Yönetimi, BGYS Proje Sorumlusu ve ilgili varlık sahipleri tarama takvimi hakkında bilgilendirilir.
- Taramalar, karşılaşılabilecek hizmet kesinti riskini en aza indirecek şekilde planlanır ve sonucunda Tarama Planı ve Kapsamı Dokümanı oluşturulur.
- Çalışan sistemlerde kesintiye sebep olacak, sistem yapılandırmalarında veya tutulan verilerde değişikliğe sebep olabilecek taramalardan zorunlu olmadıkça kaçınılır, zorunlu durumlarda bu taramalar ilgili sistem sahibi tarafından onaylanır.
- Tarama yapılacak sistemlerin taramaya hazır olmasının sağlanması ve zamanının belirlenmesi ilgili varlık sahibinin sorumluluğundadır.

3.1.2 Dış Taraflarca Yapılan Açıklık Taraması

- Kurum içi yapılan çalışmalara ek olarak, bağımsız ve yetkin kurum/kuruluş tarafından teknik açıklıkların tespiti amacıyla hizmet alımı yapılabilir. Alınan hizmet kapsamında sistem açıklık raporu hazırlanır ve gerekli aksiyonların alınması için ilgili ekiplere bilgilendirme yapılır. Bu durumda Bilgi İşlem Daire Başkanlığı tarafından;
    - Test kapsamı ve testi yapılacak sistemlerin gerekli bilgileri belirlenir.
    - Sızma testi ve/veya açıklık taramasını yapacak firma çalışanlarının yetkinlik belgeleri istenir.
    - Sızma testi ve/veya açıklık taraması için iş planları ve kullanacakları araçların listesi istenir. Kullanılacak açıklık tarama araçlarının sektörde kabul görmüş lisanslı araçlar olup olmadığı kontrol edilir.
    - Yapılacak çalışmanın takvimi hakkında Kurum Yönetimi bilgilendirilir.
    - Çalışmayı yapacak firma çalışanlarına test ve taramalar için kullanıcı hesabı oluşturulur. Tarama bitiminde kullanıcı hesapları pasif hale getirilir.
    - Teknik açıklık taramalarının karşılıklı gizliliğini sağlamak amacıyla gerekli eklemelerle Gizlilik Sözleşmesi (NDA) imzalanır. Çalışmayı yapacak firma çalışanlarının kullanımı için uygun bir fiziksel bir ortam ayrılır. Bu ortamın Kurum personelinin çalışma ofislerine uzak bir noktada olması tercih edilir.

3.1.3 Raporlama

- Denetim sonucunda tespit edilen teknik zafiyetleri ve çözüm önerilerini içeren raporlar Bilgi İşlem Daire Başkanlığı'na teslim edilir, BGYS Proje Sorumlusu bilgilendirilir. BGYS Proje Sorumlusu, gerektiğinde, teknik açıklık tetkik raporunu Bilgi Güvenliği Yönetim Sistemi Ekibine sunar.
- Bilgi İşlem Daire Başkanlığı raporların güvenli ortamda saklanmasından sorumludur. Raporlar güvenli bir ortamda saklanır ve erişimler kısıtlanır.
- Denetim sırasında tespit edilen açıklıklar, etki dereceleri ve gerçekleşme ihtimallerine göre sınıflandırılır.
- Rapor, yönetici özeti ve teknik rapor bölümlerinden oluşur.
- ASB personeli, tespit edilen teknik açıklıkların belirlenmesinden sonra kuruluş ilişkili risklerin ve alınması gereken eylemlerin (Aksiyon) Risk Yönetim Prosedürü'ne göre tanımlanmasını sağlar.

3.1.4 Teknik Açıklıkların Kapatılması

- Tespit edilen açıklıkların ortadan kaldırılması için gerekli düzeltici / iyileştirici aksiyonlar. Düzeltici ve Önleyici Faaliyet Prosedürü referans alınarak, ilgili sistem sorumluları tarafından gerçekleştirilir. Yama yüklenmesi gereksinimi var ise Madde 3.1.5 Yama Yönetimi Prosedürü işletilir. İş ihtiyacı veya sistem kesintisi ihtimali sebebiyle kapatılamayacak açıklıklar için Bilgi İşlem Daire Başkanlığı'nın onayı alınır.
- Bilgi güvenliği olaylarına müdahale Log Yönetimi Politikası'na göre yapılır.

3.1.5 Yama Yönetimi Prosedürü

- İşletim sistemi güvenlik yamaları aylık rutin güvenlik güncellemeleri kapsamında kontrollü olarak yüklenir. Bu işin takibinden ilgili Bilgi İşlem Daire Başkanlığı sorumludur.
- Bilgi İşlem Daire Başkanlığı kapsamında olmayan işletim sistemlerinin ve Bilgi İşlem Daire Başkanlığı'nın işletmediği yama yönetiminden ilgili birimler sorumludur.
- Kurumsal anti-virüs ve saldırı tespit sistemi yazılım güncellemeleri iş bilgisayarlarına ve sunucu sistemlerine Bilgi İşlem Daire Başkanlığı tarafından yüklenir.

3.1.6 Sonuçların Değerlendirilmesi

- Gerekli durumlarda, BGYS Proje Sorumlusu, tarama sonuçlarını Bilgi Güvenliği Yönetim Sistemi Ekibi ile değerlendirir.
- BGYS Proje Sorumlusu ve ASB personeli teknik açıklık tetkik raporunu ve değerlendirme toplantıları sonuçları doğrultusunda tespit edilen güvenlik açıklıklarının giderilmesi için düzeltici faaliyetleri belirler ve iş birliği içinde kendi yetki alanlarına giren işler için ilgili personeli görevlendirir ve sonuçlarını takip eder.

3.1.7 Takip Denetimi

- Tespit edilen açıklıkların kapatılma durumu tekil kontroller ile takip edilir.
- Takip denetimi ihtiyaç olması durumunda gerçekleştirilir. Takip denetimi Bilgi İşlem Daire Başkanlığı tarafından yapılır.
- Takip denetimi sonrasında tespit edilen uygunsuzluklar için "Düzeltici Faaliyet" kaydı açılır.

3.2 Bilgi Sistemleri Tetkik Kontrolleri (TS ISO 27001 EK A-12.7.1)

- Bilgi Sistemleri ve veriye erişim için planlanan tetkik testlerin gereksinimleri ASB personeli tarafından onaylanır.
- Tetkik testleri sırasında testi yapan kişilere, yazılım ve veriye, sadece okunabilir erişim verilir.

- Bilgi Sistemlerinin erişilebilirliğini etkileyebilecek tetkik testleri mesai saatleri dışında yapılır.
- Bilgi sistemleri tetkik kontrolleri sırasında tüm erişimlerin ve çalışma görüntüsünün kaydı tutulur.

3.3 Teknik Uyum Gözden Geçirmesi (TS ISO 27001 EK A-18.2.3)

- Kurumda kullanılan bilgi güvenliği standartları ile bilgi sistemleri faaliyetlerinin uyumluluğu düzenli bir şekilde gözden geçirilmelidir. Teknik uyum gözden geçirmeleri sızma testleri, açıklık değerlendirmeleri gibi faaliyetleri kapsamalıdır.
- Gözden geçirmeler teknik uzman tarafından araç yardımı ile veya manuel olarak yapılmalı ve sonuçları raporlanmalıdır.

Gerekli görülen durumlarda teknik uyum gözden geçirmeleri Kurum dışı bağımsız bir firma veya uzmana yaptırılabilir, bu durumda Madde 3.1.2'de belirtilen kurallar dikkate alınmalıdır.

Üniversite Senatosu	
Karar Tarihi	**Karar Sayısı**
05.01.2028	2018/1-17
Revizyon Tarihi	**Karar Sayısı**
15.08.2023	2023/16-08
18.10.2023	2023/25-02
11.09.2025	2025/24-12