ULUSAL MESLEK STANDARDI

SİBER GÜVENLİK ANALİSTİ
SEVİYE 5

REFERANS KODU / …

RESMÎ GAZETE TARİH-SAYI/ …

Meslek:	**SİBER GÜVENLİK ANALİSTİ**
Seviye:	**5**[I]
Referans Kodu:	**…….**
Standardı Hazırlayan Kuruluş(lar):	**BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU (BTK)**
Standardı Doğrulayan Sektör Komitesi:	**MYK Bilişim Teknolojileri Sektör Komitesi**
MYK Yönetim Kurulu Onay Tarih/ Sayı:	**……. Tarih ve ……. Sayılı Karar**
Resmî Gazete Tarih/Sayı:	…
Revizyon No:	**00**

[I] Mesleğin yeterlilik seviyesi, sekizli (8) seviye matrisinde seviye (5) olarak belirlenmiştir.

TERİMLER, SİMGELER VE KISALTMALAR

ACİL DURUM: İşyerinin tamamında veya bir kısmında meydana gelebilecek yangın, patlama, tehlikeli kimyasal maddelerden kaynaklanan yayılım, doğal afet gibi acil müdahale, mücadele, ilkyardım veya tahliye gerektiren olayları,

ATAK VEKTÖRÜ: Kötü niyetli bir kullanıcının ilgili siteme sızmak için kullanabileceği tüm iletişim yolları,

BİLGİ GÜVENLİĞİ: Bilginin yetki dışı bir başka kişiye aktarılması, değiştirilmesi, tahrif edilmesi, açığa vurulması tehlikelerine karşı korunmasını, bilginin kime ait olduğunun belirlenmesi, bütünlüğünün korunması ve kullanılabilirliğinin sağlanması aşamalarını,

DONANIM: Ağ, bilgisayar veya çevre birimlerinin elektronik, elektromekanik ve mekanik aksamlardan oluşan tüm aktif cihazları,

GÜNLÜK HAREKET (İZ, LOG) Bilgisayar ya da başka bir cihaz üzerinde daha sonra irdeleme ve yorumlar yapabilmek için olaylar hakkında zaman dizinsel veriler toplamayı,

GÜRÜLTÜ: İşitme kaybına yol açan veya sağlığa zararlı olan veya başka tehlikeleri ortaya çıkaran bütün sesleri,

GÜVENLİK TESTİ: Sistem güvenliği mekanizmalarını sağladıktan sonra, sistem görevlileri dışındaki kişiler tarafından yapılan sistem açıklarını bularak, sisteme sızma testini,

GÜVENLİK YAZILIMI: Bilgisayar veya diğer ağ ve iletişim donanımlarının güvenliğini sağlamak amacıyla geliştirilmiş koruma ve anlık denetleme, izleme, yetkilendirme, raporlama yazılımlarını,

ISCO: Uluslararası Standart Meslek Sınıflamasını,

IT: Bilgi Teknolojilerini,

İSG: İş Sağlığı ve Güvenliğini,

İŞ SÜREÇLERİ YÖNETİMİ: Bir kuruluştaki bütün iş süreçlerinin, bir iş ya da bilginin evriminin otomasyona dayalı olarak gerçek zamanda izlenmesini,

KİŞİSEL KORUYUCU DONANIM (KKD): Çalışanı, yürütülen işten kaynaklanan, sağlık ve güvenliği etkileyen bir veya birden fazla riske karşı koruyan, çalışan tarafından giyilen, takılan veya tutulan, bu amaca uygun olarak tasarımı yapılmış tüm alet, araç, gereç ve cihazları,

KONFİGÜRASYON: Güvenlik sisteminin kurum ihtiyaçlarına yönelik düzenlenmesi ve kullanıma hazır hale getirilmesini,

OFİS ERGONOMİSİ: Ofis ekipmanları ve genel ofis çalışma ortamının çalışanların fiziksel ve zihinsel olarak rahat çalışmasına ve verimliliklerinin arttırılmasına yönelik olarak düzenlenmesini,

RAMAK KALA OLAY: İş yerinde meydana gelen, çalışan, iş yeri ya da ekipmanını zarara uğratma potansiyeli olduğu halde zarara uğratmayan olayı,

RİSK: Tehlikeden kaynaklanacak kayıp, yaralanma ya da başka zararlı sonuç meydana gelme ihtimalini,

RİSK DEĞERLENDİRMESİ: İşyerinde var olan ya da dışarıdan gelebilecek tehlikelerin belirlenmesi, bu tehlikelerin riske dönüşmesine yol açan faktörler ile tehlikelerden kaynaklanan risklerin analiz edilerek derecelendirilmesi ve kontrol tedbirlerinin kararlaştırılması amacıyla yapılması gerekli çalışmaları,

SIZMA: Bilişim sistemine, güvenlik önlemlerini aşarak yetkisi olmadan girmeyi,

SİBER GÜVENLİK: Bilgi ve iletişim sistemlerinin gizlilik, bütünlük, erişebilirlilik özelliklerine gelebilecek tehditlere karşı korunması yöntemlerini ve disiplinini,

SİSTEM GÜVENLİĞİ: Kurum IT altyapısının topyekûn korunmasını,

SoC: Siber Güvenlik Operasyonları Merkezi ya da Güvenlik Operasyonları Merkezi,

TEHDİT: Bilginin bozulması, bilginin ifşa edilmesi, hizmet kesintisi gibi istenmeyen durumlara neden olma potansiyeli bulunan ortamları ve olayları,

TEHLİKE: İşyerinde var olan ya da dışarıdan gelebilecek, çalışanı veya işyerini etkileyebilecek zarar veya hasar verme potansiyelini,

TERMAL KONFOR: Çalışma ortamında çalışanların büyük çoğunluğunun ısı, nem, hava akım hızı ve termal radyasyon gibi iklim şartları açısından, bedensel ve zihinsel faaliyetlerini sürdürürken belli bir rahatlık içinde bulunmasını,

TERMAL RADYASYON: İletimi için maddesel bir ortama gerek olmayan ısı türünü,

ULUSAL GÜVENLİK NORMLARI: Kurumun konumlandığı bölge ve kurumun faaliyet konusu açısından tanımlanmış en az güvenlik gerekliliklerinin tanımlarını,

ULUSAL GÜVENLİK STRATEJİLERİ: Ulusal güvenlik beklentilerine ulaşabilmek için belirlenmiş eylem planlarını,

YAZILIM: Bilgisayar ve ağ donanımsal yapısının amaca uygun şekilde kullanılmasını sağlayan komutlar topluluğunu,

ZAFİYET: Kendi başına bir zarar vermeyen ama tehditlerin suiistimal edebileceği zayıflıkları,

ZAFİYET ANALİZİ: İşletmenin/kurumun zafiyetlerini ortaya koymak için yapılan bir dizi işlemler silsilesini

ifade eder.

İÇİNDEKİLER

1. GİRİŞ

Siber Güvenlik Analisti (Seviye 5)), Ulusal Meslek Standardı 19/10/2015 tarihli ve 29507 sayılı Resmî Gazete'de yayımlanan Ulusal Meslek Standartlarının ve Ulusal Yeterliliklerin Hazırlanması Hakkında Yönetmelik ve 27/11/2007 tarihli ve 26713 sayılı Resmî Gazete'de yayımlanan Mesleki Yeterlilik Kurumu Sektör Komitelerinin Kuruluş, Görev, Çalışma Usul ve Esasları Hakkında Yönetmelik hükümlerine göre MYK'nın görevlendirdiği Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanmış sektördeki ilgili kurum ve kuruluşların görüşleri alınarak değerlendirilmiş ve MYK Bilişim Teknolojileri Sektör Komitesi tarafından incelendikten sonra MYK Yönetim Kurulunca onaylanmıştır.

2. MESLEK TANITIMI

2.1. Meslek Tanımı

Siber Güvenlik Analisti (Seviye 5), iş sağlığı ve güvenliği ile çevre koruma önlemlerini uygulayarak kalite gereklilikleri çerçevesinde, mesleği ile ilgili iş organizasyonu yapan, işletmelerin ve/veya Kurumların bilişim altyapısı siber güvenlik ihtiyaçlarını belirleyen, siber olay yönetim organizasyonunu gerçekleştiren, siber güvenlik analizi çalışmalarına katılan ve mesleki gelişim çalışmalarına katılan nitelikli kişidir.

2.2. Mesleğin Uluslararası Sınıflandırma Sistemlerindeki Yeri

ISCO 08: 2529 (Başka yerde sınıflandırılmamış veri tabanı ve bilgisayar ağları ile ilgili profesyonel meslek mensupları)

2.3. Sağlık, Güvenlik ve Çevre ile ilgili Düzenlemeler

2872 sayılı Çevre Kanunu ve yürürlükteki alt mevzuatı.
4857 sayılı İş Kanunu ve yürürlükteki alt mevzuatı.
5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve yürürlükteki alt mevzuatı.
6331 sayılı İş Sağlığı ve Güvenliği Kanunu ve yürürlükteki alt mevzuatı.
Ambalaj Atıklarının Kontrolü Yönetmeliği
Elektrik Tesislerinde Topraklamalar Yönetmeliği
Kişisel Koruyucu Donanım Yönetmeliği
Makina Emniyeti Yönetmeliği
Ayrıca, iş sağlığı ve güvenliği ve çevre ile ilgili yürürlükte olan diğer mevzuata uyulması ve konu ile ilgili risk değerlendirmesi yapılması esastır.

2.4. Meslek ile İlgili Diğer Mevzuat

5070 sayılı Elektronik İmza Kanunu ve yürürlükteki alt mevzuatı.
5237 sayılı Türk Ceza Kanunu ve yürürlükteki alt mevzuatı.
5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve yürürlükteki alt mevzuatı.
5809 sayılı Elektronik Haberleşme Kanunu ve yürürlükteki alt mevzuatı.
TSE/ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
Ayrıca, meslek ile ilgili yürürlükte diğer mevzuata uyulması esastır.

2.5. Çalışma Ortamı ve Koşulları

Siber Güvenlik Analisti (Seviye 5), genelde kapalı alanlarda, iyi aydınlatılmış, havalandırılmış, termal konfor koşulları ve uygun gürültü düzeyinde, ofis ergonomisine uygun hazırlanmış ortamlarda ayakta veya oturarak çalışır. SoC merkezlerinde vardiya durumu olabilir. Veri merkezleri gürültülü ve soğuk olabilir. Birlikte çalıştığı kişiler ilgili birim amirleri ve çalışma arkadaşlarıdır.

Mesleğin icrası esnasında iş sağlığı ve güvenliği önlemlerini gerektiren kaza, yaralanma, tahriş ve zehirlenme riskleri bulunmaktadır. Bu risklerin tamamen bertaraf edilmesi ve önlenebilmesi için işveren tarafından gerekli önlemler alınır. Risklerin tamamen ortadan kaldırılamadığı durumlarda toplu koruma önlemlerine uygun olarak çalışır, eğer toplu koruma önlemleri uygulanamıyorsa işveren tarafından sağlanan uygun kişisel koruyucu donanımı kullanarak çalışır.

2.6. Mesleğe İlişkin Diğer Gereklilikler

Mesleğe ilişkin diğer gereklilikler bulunmamaktadır.

3. MESLEK PROFİLİ

3.1. Görevler, İşlemler ve Başarım Ölçütleri

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
A	İş süreçlerinde İSG, çevre koruma ve kalite prosedürlerini uygulamak (devamı var)	**A.1**	İSG prosedürlerini uygulamak	**A.1.1**	Üretim ortamında, İSG talimatlarına göre, kendisini ve çevresindekileri riske atmayacak şekilde çalışır.
				A.1.2	Üretim ortamındaki makine, araç, gereç ve diğer üretim araçları ile bunların güvenlik donanımlarını sağlık ve güvenlik işaretlerine ve talimatlara uygun şekilde kullanır.
				A.1.3	Üretim ortamında, iş süreçlerine göre KKD'leri talimatlarına uygun olarak kullanır.
				A.1.4	Kendisini ve çevresini etkileyeceğini gözlemlediği tehlike, risk ve ramak kala olayları yazılı ve/veya sözlü olarak ilgililer ile paylaşır.
				A.1.5	Risk değerlendirmesi çalışmalarında gözlem ve görüşlerini risk değerlendirmesi ekibine iletir.
				A.1.6	Risk arz eden çalışmalarda, talimata uygun önlemleri uygular.
		A.2	Acil durum prosedürlerini uygulamak	**A.2.1**	Acil durum planında belirtilen hususlar dâhilinde alınan önleyici ve sınırlandırıcı tedbirlere uyar/uyulmasını sağlar.
				A.2.2	İşyerinde sağlık ve güvenlik hususlarında karşılaştığı acil durumları ilgili kişilere iletir.

Görevler		İşlemler		Başarım Ölçütleri	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
A	İş süreçlerinde İSG, çevre koruma ve kalite prosedürlerini uygulamak	**A.3**	Çevre koruma prosedürlerini uygulamak	**A.3.1**	Üretim ortamında, olası çevre tehlike ve risklerinin tespit ve takibi ile ilgili çalışmalara destek verir.
				A.3.2	İş süreçlerinde ortaya çıkan atık malzeme (kablolar ve benzeri) ile elektronik atıkların tasnif ve bertarafına yönelik prosedürleri uygular.
		A.4	Kalite ve verimlilik çalışmalarına katılmak	**A.4.1**	İş süreçlerindeki hataların kök nedenlerini belirler/belirlenmesine katkıda bulunur.
				A.4.2	Üretim süreçlerindeki kalite çalışmalarına kendi görev alanı dahilinde katılır.

Görevler		İşlemler		Başarım Ölçütleri	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
B	İş organizasyonu yapmak (devamı var)	**B.1**	İş planlaması yapmak	**B.1.1**	İşletme yöntem, kural ve formatlarına uygun olarak iş emirlerini sistemden/ilgili birimden/amirden alarak gelen iş emrine yönelik ilgili kaynaklardan bilgi toplar.
				B.1.2	Aldığı iş emirlerine ve topladığı bilgilere göre yapılacak faaliyetlerin sınıflamasını ve sıralamasını yaparak tahmini işlem sürelerini saptar.
				B.1.3	İş emrine konu olan bilgisayar donanımlarının özelliklerine ve ortam koşullarına göre, uygun çalışma alanının (donanımların bulunduğu alan veya özel atölye) neresi olduğuna karar verir.
				B.1.4	Yaptığı sıralama ve belirlediği tahmini işlem sürelerini esas alarak eldeki iş gücü ve zaman kapasitesine göre işletme formatına uygun şekilde iş planını yaparak amirine onaylatır.
				B.1.5	İş planını gerektiğinde, değişen koşullara ve amirin yönlendirmesine göre revize eder.
				B.1.6	İş programına ve iş emirlerine göre personeli yönlendirerek işlemlerin gerçekleştirilmesini sağlar.
		B.2	Faaliyetler için araç, gereç ve donanım temin etmek	**B.2.1**	İş süreçlerinde kullanacağı ekipman ve malzemelerin ön kontrollerini yapar/yapılmasını sağlar.
				B.2.2	İş süreçlerinde kullanacağı ekipmanların kalibrasyon takibini yapar.
				B.2.3	Çalışma için gerekli donanım, malzeme ve ekipmanları çalışmaya hazır hale getirir.
		B.3	Yapılan işlerin kaydını tutmak	**B.3.1**	İş emri, süreç, fire/hata, ölçüm gibi formları işletme formatlarına uygun olarak doldurur.
				B.3.2	Kendisine bağlı ekiplerin doldurduğu formları kontrol eder.
				B.3.3	Doldurulan iş emri ve diğer formları varsa ilgili dijital sisteme girerek amirlerin kontrol ve onayına sunar.
				B.3.4	Amirin kontrol ve onayı sonrasında, formları varsa ilgili birimlere iletir.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
B	İş organizasyonu yapmak	**B.4**	Dijital arşivleme yaptırmak	**B.4.1**	İş süreçlerinde kullanılacak yazılımların güvenli ve güncel olarak bulundurulmasını sağlar.
				B.4.2	İş süreçleri sonunda oluşan rapor, form ve benzeri kaynak materyallerin sonraki düzeylerde teknik aktarım amacıyla işletme kural ve yöntemlerine uygun olarak arşivlenmesini sağlar.
				B.4.3	Dijital arşivin güvenlik ve koruma önlemlerini işletme kural ve yöntemlerine göre uygular.
		B.5	Çalışma alanının düzenini takip etmek	**B.5.1**	Çalışmaların kesintisiz ve uygun şekilde sürdürülmesi için, çalışma alanını inceleyerek özelliklerini ve çalışma noktalarının kapsamını belirler.
				B.5.2	Çalışma alanının, kapsamına ve belirlenen özelliklerine göre, emniyet ve teknik olarak yapılacak işe uygun ortam koşullarına getirilmesini sağlar.
				B.5.3	Çalışma alanı içerisinde işiyle ilgili olmayan malzemeleri ortamdan uzaklaştırır veya uzaklaştırılmasını sağlar.
				B.5.4	Çalışma alanı ile ilgili araç, gereç ve takımların yerlerini tanımlayarak yerlerinde bulundurur.
				B.5.5	Çalışma alanında kullanılmayan elektrikli araç, gereç ve takımların elektriğini keser.
				B.5.6	Çalışma sonunda, çalışma sahasını işin özelliklerine, etkisine ve bunlarla ilgili yöntemlere göre temizleyerek düzenler.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
C	Bilişim altyapısı siber güvenlik ihtiyaçlarını belirlemek	**C.1**	Bilgi sistemleri envanteri oluşturmak	**C.1.1**	Kullanılan ağ ve güvenlik cihazları ile işletim sistemleri ve servisler hakkında bilgi toplar.
				C.1.2	Topladığı bilgiler doğrultusunda marka/model/sürüm gibi belirleyici bilgilerin raporlamasını yapar.
				C.1.3	Kullanılan bilgi sistemleri envanterini oluşturarak, bilgileri güncel tutar.
				C.1.4	Bilgi sistemleri envanterini sorumlu birimlerle ilişkilendirerek raporlamasını yapar.
		C.2	Zafiyet yönetimi yapmak	**C.2.1**	Kullanılan bilgi sistemlerinde çıkan zafiyet ve olayları takip eder.
				C.2.2	Gerçekleştirilen güvenlik testleri sonuçlarını inceler.
				C.2.3	Zafiyetleri ilgili birimlere iletir.
				C.2.4	Zafiyetin giderilip giderilmediğini belirli aralıklarla kontrol eder.
				C.2.5	Zafiyetlerin durumlarını ilgili birim ve mercilere raporlar.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
D	Siber olay yönetim organizasyonunu gerçekleştirmek	**D.1**	Terminoloji ve atak vektörleri hakkında güncellemeleri yapmak	**D.1.1**	Siber güvenlik (İnternet, İntranet, Mobil, DDoS ve benzeri) atak vektörler ile ilgili kaynak araştırması yaparak, varsa güncel bilgileri teknik ekibe bildirir.
				D.1.2	İşletim sistemi ve uygulama iz kayıtları incelemeleri hakkında kaynak araştırması yaparak, varsa güncel bilgileri teknik ekibe bildirir.
		D.2	Siber olay kaynaklarını incelemek	**D.2.1**	Bilgi sistemleri kaynaklarının durumunu kontrol eder.
				D.2.2	Kullanılan cihaz, servis ve uygulamaların erişilebilirliğini ve yükünü takip eder.
				D.2.3	Bilgi sistemleri kaynaklarından alınan iz kayıtlarını inceler.
				D.2.4	İncelenen iz kayıtlarını ilişkilendirir, zenginleştirerek anlamlandırır.
		D.3	Olay değerlendirmesini yapmak	**D.3.1**	İlişkilendirilen iz kayıtlarından alarm oluşturur.
				D.3.2	Sistem tarafından oluşturulan alarmları değerlendirir.
				D.3.3	İhbar olarak gelen alarm ve olası olayları değerlendirilir.
				D.3.4	İncelemeler doğrultusunda olay oluşturur
				D.3.5	Gerekli iz kayıtları, dosyalar ve diğer bilgileri toplayarak, siber olay formunu doldurur.
		D.4	Siber olay için aksiyon belirlemek	**D.4.1**	Siber olay tespiti kesin, alınması gereken aksiyon belli ise, olayı sistem sahipleri ve bildirim yapılması gereken diğer birim ve mercilere bildirir.
				D.4.2	Siber olayın tespiti veya alınacak aksiyon ile ilgili netleşmesi gereken konular var ise, ileri derece analiz ve inceleme için diğer birimlere kaynakları iletir.
				D.4.3	Yapılan bildiri ve iletilen bilgiler ile ilgili aksiyon formunu doldurur.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
D	Siber olay yönetim organizasyonunu gerçekleştirmek	**D.5**	Aksiyon takibi yapmak	**D.5.1**	Siber olayın devam edip etmediğinin takibini belirli aralıklarla yapar.
				D.5.2	İleri inceleme ve analiz çalışmaları sonucuyla ilgili bildirimleri ilgili birimlere yapar.
				D.5.3	Yapılan çalışmanın raporlamasını yapar.
		D.6	Siber güvenlik farkındalığı oluşturmak	**D.6.1**	Kurum/firma içindeki ve globaldeki bilgi güvenliği politikalarını ve güncellemeleri inceler.
				D.6.2	İncelenen politika ve güncel bilgiler doğrultusunda farkındalık çalışmaları planlar.
				D.6.3	Farkındalık çalışmaları kapsamında, bilgi güvenliği temelleri ile ilgili bilgileri personele ulaştırır.
				D.6.4	E-posta, bildiri, poster vb. yöntemler kullanarak güvenlik uyarılarını personele bildirir.
				D.6.5	Personel farkındalığını arttırmak için sosyal mühendislik çalışmaları planlar ve gerçekleştirir.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
E	Siber güvenlik analizi çalışmalarına katılmak	**E.1**	Kullanılan sistemin çalışma ve sürdürülebilirliğini takip etmek	**E.1.1**	Sistem üzerinde incelenen tüm kaynaklardan veri alındığının kontrolünü yapar.
				E.1.2	Sistem kaynakların kullanım oranlarını takip eder.
				E.1.3	Sistem üzerinde oluşturulan alarm kurallarını inceleyerek düzenler.
				E.1.4	Güncel bilgilere göre sistem üzerinde yeni alarm kuralları girer.
		E.2	İleri inceleme ve analiz çalışmalarına destek vermek	**E.2.1**	Olay müdahale aksiyonlarının belirlenmesi ve düzenlenmesini sağlar.
				E.2.2	Güvenlik testi çalışmalarına katkı vererek; kapsam belirleme, gerekli izinlerin tanımlanması, sistemlerin işleyişi ve çalışmanın sağlıklı devam edebilmesi için gerekli kontrollerin yapılmasında görev alır.
				E.2.3	Zararlı yazılım analizi süreçlerine katkı vererek; zararlı yazılımın tespiti, bulunması, muhafaza edilmesi, iletilmesi ve karşı aksiyonların alınması konularında görev alır.
				E.2.4	Adli bilişim sürecini yöneten ekibe katkı vererek; imaj alma, verinin saklanması, iletilmesi ve oluşturulacak zaman çizelgesi hazırlanması konularında görev alır.

Görevler		İşlemler		Başarım Ölçütleri	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
F	Mesleki gelişim çalışmalarına katılmak	**F.1**	Kişisel mesleki gelişimini sağlamak	**F.1.1**	Sektörel gelişmeleri ve gelişim sağlayan aktiviteleri takip eder.
				F.1.2	Kariyer hedeflerine yönelik eğitimler, çalışmalar ve faaliyetlere katılarak mesleki portföyünü oluşturur.
		F.2	Ekibin mesleki gelişimini desteklemek	**F.2.1**	Ekip elemanlarının eğitim ve gelişim ihtiyaçlarını tespit ederek ilgili birime iletir.
				F.2.2	Yeni elemanların yetişmeleri ve yetkin olmalarına iş süreçleri kapsamında destek verir.

3.2. Kullanılan Araç, Gereç ve Ekipman

1. Belgegeçer ve fotokopi makinesi
2. Bilgisayar çevre birimleri (yazıcı, barkod okuyucu, tarayıcı, ve benzeri)
3. Bilgisayar ekranı (CRT, LCD, LED)
4. Çeşitli güvenlik tarayıcı yazılımlar ve raporlama araçları
5. Depolama ortamları (CD, DVD, disket, vb.)
6. Dijital görüntüleme donanımları (webcam, fotoğraf makinesi, kamera ve benzeri)
7. Dönüştürücüler (DVI, HDMI, PATA, USB)
8. Güvenlik, tanımlama, sorun giderme ve veri kurtarma araçları
9. Harici depolama birimleri (flash bellek, HDD)
10. Her türlü güvenlik duvarı, ağ aktif cihazları, ağ yönetim yazılımları
11. Ağ bağlantılı bilgisayar
12. İlkyardım malzemeleri
13. İşletim sistemleri ve ofis yazılımları
14. Kablolu ve kablosuz iletişim araçları (telefon, cep telefonu, telsiz, ses kayıt cihazı, ve benzeri)
15. Kesintisiz güç kaynağı (UPS)
16. Kişisel koruyucu donanım
17. Ofis ve kırtasiye malzemeleri
18. Virüs, casus yazılım, solucan ve benzeri sistemi tehdit eden tehlikeleri tespit eden virüs koruma yazılımları
19. Yangın söndürme tüpü

3.3. Bilgi ve Beceriler

1. Analitik düşünme becerisi
2. Basit ilkyardım bilgisi
3. Bilgi güvenliği yönetim sistemi standartları ve uygulama teknikleri bilgisi
4. Bilgisayar donanımları ve çevre birimleri bilgisi
5. Çevre koruma yöntemleri ve yasal düzenlemeler bilgisi
6. Ağ teknolojileri bilgisi
7. Doğal kaynakların etkin kullanımı bilgisi
8. Ekip yönetimi becerisi
9. Genel iş sağlığı ve güvenliği bilgisi
10. Güvenli ağ ve internet bağlantısı kurulum bilgisi ve uygulama becerisi
11. Güvenlik donanım araç ve gereçleri bilgisi
12. Güvenlik teknolojileri temel kullanım bilgisi ve uygulama becerisi
13. İş organizasyonu ve planlama becerisi
14. İşletim sistemleri ve sunucu yazılımları bilgisi
15. Kimlik ve kaynak yönetimi bilgisi
16. Kriz yönetimi bilgi ve becerisi
17. Mesleğe ilişkin yasal düzenlemeler bilgisi

18. Mesleki matematik, terim ve yabancı dil bilgisi
19. Öğrenme ve öğrendiğini aktarabilme yeteneği
20. Programlama bilgisi
21. Risk yönetimi bilgi ve becerisi
22. Sektöre ait ulusal ve uluslararası standartlar bilgisi
23. Sistem ve uygulama yazılımları bilgisi
24. Şifreleme ve algoritma bilgisi
25. Teknik dokümanları okuma ve anlama bilgi ve becerisi
26. Temel çalışma mevzuatı bilgisi
27. Veri tabanı güvenliği bilgi ve becerisi
28. Veri toplama, kayıt tutma ve raporlama bilgi ve becerisi
29. Yangın önleme, yangınla mücadele, acil durum ve tahliye bilgisi
30. Yazılı ve sözlü iletişim yeteneği
31. Zaman yönetimi bilgisi

3.4. Tutum ve Davranışlar

1. Acil ve stresli durumlarda soğukkanlı ve sakin olmak
2. Amirlerine doğru ve zamanında bilgi aktarmak
3. Araç, gereç ve ekipmanların kullanımına özen göstermek
4. Çalışma zamanını iş emrine uygun şekilde etkili ve verimli kullanmak
5. Çevre, kalite ve İSG mevzuatında yer alan düzenlemeleri benimsemek
6. Çevreyi korumaya karşı duyarlı olmak
7. Deneyimlerini iş arkadaşlarına aktarmak
8. İşletme kaynaklarının kullanımı ve geri kazanım konusunda duyarlı olmak
9. İşyeri çalışma prensiplerine uymak
10. İşyeri hiyerarşi ilişkisine uygun hareket etmek
11. İşyeri prosedür ve talimatlarına uygun davranmak
12. Kendisinin ve diğer kişilerin güvenliğini gözetmek
13. Mesleki gelişim için araştırmaya istekli olmak
14. Risk değerlendirmesinde belirtilen hususlar ile İSG kurallarına riayet etmek
15. Risk faktörleri konusunda duyarlı olmak
16. Sorumluluklarını zamanında yerine getirmek
17. Tehlike durumlarında ilgilileri zamanında bilgilendirmek
18. Temizlik, düzen ve işyeri tertibine özen göstermek
19. Vardiya değişimlerinde etkili, açık ve doğru şekilde bilgi paylaşmak
20. Yeniliklere açık olmak ve değişen koşullara uyum sağlamak

4. ÖLÇME, DEĞERLENDİRME VE BELGELENDİRME

Siber Güvenlik Personeli (Seviye 5) meslek standardını esas alan ulusal yeterliliklere göre belgelendirme amacıyla yapılacak ölçme ve değerlendirme, gerekli şartların sağlandığı ölçme ve değerlendirme merkezlerinde yazılı ve/veya sözlü teorik ve uygulamalı olarak gerçekleştirilecektir.

Ölçme ve değerlendirme yöntemi ile uygulama esasları bu meslek standardına göre hazırlanacak ulusal yeterliliklerde detaylandırılır. Ölçme ve değerlendirme ile belgelendirmeye ilişkin işlemler 15/10/2015 tarihli ve 29503 sayılı Resmî Gazete'de yayımlanan Mesleki Yeterlilik Kurumu, Sınav, Ölçme, Değerlendirme ve Belgelendirme Yönetmeliği çerçevesinde yürütülür.

Not: Bu kısım Resmi Gazete'de yayımlanmayacaktır. Sadece MYK web sitesinde yer alacaktır.

Ek: Meslek Standardı Hazırlama Sürecinde Görev Alanlar

1. Meslek Standardı Hazırlayan Kuruluşun Meslek Standardı Ekibi:

Onur AKTAŞ	Bilgi Teknolojileri ve İletişim Kurumu, Mühendis
Mustafa Kaan İLTER	Bilgi Teknolojileri ve İletişim Kurumu, Mühendis
Emre MÜLAZIMOĞLU	Bilgi Teknolojileri ve İletişim Kurumu, Mühendis
Fatih ÖZKUL	Bilgi Teknolojileri ve İletişim Kurumu, Mühendis
Zeynep GÜRLÜK	Bilgi Teknolojileri ve İletişim Kurumu, Mühendis
Harun DEMİR	Sanayi ve Teknoloji Bakanlığı, Sanayi ve Teknoloji Uzmanı

2. Görüş İstenen Kişi, Kurum ve Kuruluşlar:

- Aile, Çalışma ve Sosyal Hizmetler Bakanlığı (İş Sağlığı ve Güvenliği Genel Müdürlüğü)
- MEB Mesleki ve Teknik Eğitim Genel Müdürlüğü
- MEB Hayat Boyu Öğrenme Genel Müdürlüğü
- MEB Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
- İç İşleri Bakanlığı (Emniyet Genel Müdürlüğü)
- Türkiye İş Kurumu (İş ve Meslek Danışmanlığı Dairesi Başkanlığı)
- Türkiye İstatistik Kurumu (TÜİK)
- Yükseköğretim Kurulu Başkanlığı (YÖK)
- Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı
- Türkiye İhracatçılar Meclisi (TİM)
- Türkiye Odalar ve Borsalar Birliği (TOBB)
- Türkiye Esnaf ve Sanatkârları Konfederasyonu (TESK)
- Hak-İş Konfederasyonu
- Türkiye İşçi Sendikaları Konfederasyonu (TURK-İŞ)
- Türkiye İşveren Sendikaları Konfederasyonu (TİSK)
- Ankara Sanayi Odası (ASO)
- Ankara Ticaret Odası (ATO)
- İstanbul Ticaret Odası (İTO)
- Ege Bölgesi Sanayi Odası (EBSO)
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
- Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Yüksek Lisans Programı
- Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği
- Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Anabilim Dalı

- Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Siber Güvenlik Yüksek Lisans Programı
- Hacettepe Üniversitesi Bilişim Enstitüsü Bilgi Güvenliği Anabilim Dalı
- Işık Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Yüksek Lisans Programı
- İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Anabilim Dalı
- İstanbul Teknik Üniversitesi Bilişim Enstitüsü Bilişim Uygulamaları Anabilim Dalı Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programı
- Kadir Has Üniversitesi Siber Güvenlik ve Kritik Altyapı Koruma Uygulama ve Araştırma Merkezi
- Milli Savunma Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı Siber Güvenlik Yüksek Lisans Programı
- Ortadoğu Teknik Üniversitesi Enformatik Enstitüsü Siber Güvenlik Anabilim Dalı
- Sabancı Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi Siber Güvenlik Lisansüstü Programı
- Süleyman Demirel Üniversitesi Mühendislik Mimarlık Fakültesi Uzaktan Eğitim Bilgisayar Mühendisliği Siber Güvenlik Tezsiz Yüksek Lisans
- İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı
- TOBB ETÜ Fen Bilimleri Enstitüsü Siber Güvenlik Lisans Üstü Programı
- ASELSAN
- HAVELSAN
- STM
- NETAŞ
- TÜRK TELEKOM
- TURKCELL
- VODAFONE
- Türkiye Bilişim Derneği
- Bilgi Güvenliği Derneği
- Kamu Siber Güvenlik Derneği
- Bilişim Teknolojileri ve Siber Güvenlik Derneği
- Uluslararası Siber Güvenlik Federasyonu

3. MYK Sektör Komitesi Üyeleri ve Uzmanlar

.

.

.

4. MYK Yönetim Kurulu

Adem CEYLAN	Aile, Çalışma ve Sosyal Hizmetler Bakanlığı Temsilcisi, Başkan
Prof. Dr. Mehmet SARIBIYIK	Yükseköğretim Kurulu Temsilcisi, Başkan Vekili
Dr. Recep ALTIN	Milli Eğitim Bakanlığı Temsilcisi, Üye
Bendevi PALANDÖKEN	Meslek Kuruluşları Temsilcisi, Üye
Dr. Osman YILDIZ	İşçi Sendikaları Konfederasyonları Temsilcisi, Üye
Celal KOLOĞLU	İşveren Sendikaları Konfederasyonu Temsilcisi, Üye