ULUSAL MESLEK STANDARDI

SİBER GÜVENLİK ELEMANI
SEVİYE 5

REFERANS KODU / 19UMS0740-5

RESMÎ GAZETE TARİH-SAYI/ 09.02.2020 - 31034

Meslek:	**SİBER GÜVENLİK ELEMANI**
Seviye:	**5**[I]
Referans Kodu:	**19UMS0740-5**
Standardı Hazırlayan Kuruluş(lar):	**Bilgi Teknolojileri ve İletişim Kurumu (BTK)**
Standardı Doğrulayan Sektör Komitesi:	**MYK Bilişim Teknolojileri Sektör Komitesi**
MYK Yönetim Kurulu Onay Tarih/ Sayı:	**13.11.2019 tarih ve 2019/147 sayılı Karar**
Resmî Gazete Tarih/Sayı:	**9/2/2020 - 31034**
Revizyon No:	**00**

[I] Mesleğin yeterlilik seviyesi, 8 seviyeli Türkiye Yeterlilikler Çerçevesine göre 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 sisteme sızmak için kullanabileceği tüm iletişim yollarını,

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

BT: Bilgi Teknolojilerini,

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

GÜVENLİK TESTİ: Bir BT sisteminin sahip olduğu güvenlik mekanizmalarının kusurlarını ortaya çıkarmaya yönelik dışarıdan bir kullanıcı tarafından yapılan inceleme ve tetkik sürecini (zafiyet tarama, yazılım güvenlik testi, sızma testi ve benzeri),

ISCO: Uluslararası Standart Meslek Sınıflamasını,

İSG: İş Sağlığı ve Güvenliğini,

İZ KAYDI: Sunucu ve istemci bilgisayarlar ile ağ cihazları gibi donanımlarda gerçekleşen olayların (bilgi, uyarı, hata, hata ayıklama ve iz gibi) yapısal diğer bilgilerle beraber zaman bilgisi ile tutulan kayıtları,

KİŞİSEL KORUYUCU DONANIM (KKD): Çalışanı, yürütülen işten veya çalışma ortamından 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,

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: İşyerinde meydana gelen, çalışan, iş yeri ya da ekipmanını zarara uğratma potansiyeli olduğu halde zarara uğratmayan olayı,

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,

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

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

SİBER GÜVENLİK: BT sistemlerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin, olası ve güncel tehditlerin değerlendirildiği bir risk yönetimi ile en iyi uygulamalar çerçevesinde sağlanmasını,

SGOM: Siber Güvenlik Operasyonları Merkezi ya da Güvenlik Operasyonları Merkezini,

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,

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

ZAFİYET: Yazılım, donanım ve insan etmenlerinde öngörülen işlevin yerine getirilmesini engellemeyen ancak saldırı başlatmak ve yürütmek için tehditler tarafından sömürülebilecek kusurları,

ifade eder.

İÇİNDEKİLER

1. GİRİŞ

Siber Güvenlik Elemanı (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 Elemanı (Seviye 5), iş sağlığı ve güvenliği ile çevre koruma önlemlerini uygulayarak kalite gereklilikleri çerçevesinde iş yeri bilişim altyapılarının siber tehdit unsurlarına karşı korunması amacıyla, işyerinde bilgi sistemleri envanterini oluşturma, zafiyet takibi yapma ve siber güvenlik farkındalığı oluşturma işlemleri kapsamında siber güvenlik önleyici faaliyet çalışmalarına; terminoloji ve atak vektörleri hakkında güncelleme yapma, siber olay kaynaklarını inceleme, aksiyon belirleme ve aksiyon takibi yapma gibi faaliyetler doğrultusunda siber olay yönetim sürecine; siber güvenlik analizlerinde kullanılan sistemlerin çalışma ve sürdürülebilirliğini takip etme ve ileri düzey inceleme ve analiz çalışmalarına destek verme işlemleri kapsamında siber güvenlik risk analizi ve yönetimi çalışmalarına katılan ve mesleki gelişim çalışmalarını yürüten nitelikte 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 İlgili 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.
21/8/2001 tarihli ve 24500 sayılı Resmî Gazete'de yayımlanan Elektrik Tesislerinde Topraklamalar Yönetmeliği.
3/3/2009 tarihli ve 27158 sayılı Resmî Gazete'de yayımlanan Makina Emniyeti Yönetmeliği (2006/42/AT).
27/12/2017 tarihli ve 30283 sayılı Resmî Gazete'de yayımlanan Ambalaj Atıklarının Kontrolü Yönetmeliği.
1/5/2019 tarihli ve 30761 sayılı Resmî Gazete'de yayımlanan Kişisel Koruyucu Donanım 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.
6698 sayılı Kişisel Verilerin Korunması 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 Elemanı (Seviye 5), genelde kapalı alanlarda, iyi aydınlatılmış, havalandırılmış, termal konfor, gürültü düzeyi ve ofis ergonomisi şartları uygun ofislerde veya Siber Güvenlik Operasyonları Merkezleri (SGOM), veri merkezleri, sistem odaları gibi gürültülü ve soğuk yerlerde, vardiyalı veya vardiyasız şekilde, oturarak veya ayakta diğer analist ve amirleriyle birlikte çalışır.

Mesleğin icrası esnasında iş sağlığı ve güvenliği önlemlerini gerektiren kaza, yaralanma riskleri ve meslek hastalığına neden olabilecek riskler 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**	Çalışma ortamında, İSG talimatlarına göre, kendisini ve çevresindekileri riske atmayacak şekilde çalışır.
				A.1.2	Çalışma ortamındaki makine, araç, gereç ve diğer çalışma araçları ile bunların güvenlik donanımlarını sağlık ve güvenlik işaretlerine ve talimatlara uygun şekilde kullanır.
				A.1.3	Çalışma 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 çalışma yapar.
		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**	Çalışma 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	İş süreçlerindeki kalite çalışmalarına kendi görev alanı dâhilinde 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 yöneticinin bilgisi dâhilinde ilgili personele bilgi vererek işlemlerin gerçekleştirilmesini sağlar.
		B.2	Faaliyetler için yazılım, donanım ve ekipman temin etmek	**B.2.1**	İş süreçlerinde kullanacağı ekipman ve yazılımların ön kontrollerini yapar/yapılmasını sağlar.
				B.2.2	Çalışma için gerekli yazılım, donanım 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	Kendisiyle ilişkili 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 yapmak	**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 sonunda, çalışma sahasını işin özelliklerine, etkisine ve bunlarla ilgili yöntemlere göre temizleyerek düzenler.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
C	Siber güvenlik önleyici faaliyet çalışmalarına katılmak	**C.1**	Bilgi sistemleri envanteri oluşturmak	**C.1.1**	Kullanılan ağ ve güvenlik cihazları, uygulamalar, işletim sistemleri, servisler ve diğer bilişim alt yapısına yönelik sistemler 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 takibi yapmak	**C.2.1**	Kullanılan bilgi sistemlerinde çıkan zafiyet ve olayları takip eder.
				C.2.2	Gerçekleştirilen güvenlik testleri sonuçlarını inceler.
				C.2.3	Tespit edilen zafiyetlerle ilgili seviyelerini de içeren detaylı bilgileri ve zafiyetin giderilmesi için alınması gereken aksiyonları sorumlu birimlere iletir.
				C.2.4	Zafiyetin giderilip giderilmediğini belirli aralıklarla kontrol eder.
				C.2.5	Zafiyetlerin durumlarını ilgili birim ve mercilere raporlar.
		C.3	Siber güvenlik farkındalığı oluşturmak	**C.3.1**	Kurum/firma içindeki bilgi güvenliği politikalarını ve güncellemeleri inceler.
				C.3.2	İncelenen politika ve güncel bilgiler doğrultusunda farkındalık çalışmaları planlar.
				C.3.3	Farkındalık çalışmaları kapsamında, bilgi güvenliği temelleri ile ilgili bilgileri ilgili personele ulaştırır.
				C.3.4	E-posta, bildiri, poster ve benzeri yöntemler kullanarak güvenlik uyarılarını ilgili personele bildirir.
				C.3.5	İlgili personel farkındalığını arttırmak için sosyal mühendislik çalışmaları planlar ve gerçekleştirir.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
D	Siber olay yönetim sürecine katılmak (devamı var)	**D.1**	Terminoloji ve atak vektörleri hakkında güncellemeleri yapmak	**D.1.1**	Siber güvenlik (İnternet, İntranet, Mobil, DDoS ve benzeri) atak vektörleri, tedbir ve çözüm yöntemleri ile ilgili kaynak araştırması yaparak, varsa güncel bilgileri teknik ekibe bildirir.
				D.1.2	Bilgi sistemleri iz kayıtları incelemeleri hakkında kaynak araştırması yaparak, varsa güncel bilgileri teknik ekibe bildirir.
				D.1.3	Güncel bilgileri kurum iç kaynaklarında bulunan dokümantasyonlarda gerekli olması halinde günceller.
		D.2	Siber olay kaynaklarını incelemek	**D.2.1**	Bilgi sistemleri kaynaklarının güncel durumunu kontrol ederek talep edildiğinde bilgi verir.
				D.2.2	Kullanılan cihaz, servis ve uygulamaların erişilebilirliğini ve yükünü siber saldırı kapsamında takip eder.
				D.2.3	Bilgi sistemleri kaynaklarından gereli iz kayıtlarını siber güvenlik analizi için kullanılan sistemlerde toplanmasında görev alarak inceler.
				D.2.4	İncelenen iz kayıtlarını ilişkilendirerek ve zenginleştirerek anlamlandırır.
		D.3	Olay değerlendirmesi yapmak	**D.3.1**	İlişkilendirilen iz kayıtlarından rapor ve alarm oluşturur.
				D.3.2	Sistem tarafından oluşturulan alarmları değerlendirir.
				D.3.3	Dış veya iç kaynaklardan gelen alarm ve olası olayları değerlendirir.
				D.3.4	İncelemeler doğrultusunda olay bildirimi oluşturur.
				D.3.5	Gerekli iz kayıtları, dosyalar ve diğer bilgileri toplayarak, siber olay formunu doldurur.
				D.3.6	Gerektiği durumda konuyu ilgili ekiplere iletir.
				D.3.7	Gerçekleşen olayları (kötücül yazılım, veri sızıntısı ve benzeri) kategorize eder.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
D	Siber olay yönetim sürecine katılmak	**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.
		D.5	Aksiyon takibi yapmak	**D.5.1**	Siber olayın devam edip etmediğinin takibini belirli aralıklarla yapar.
				D.5.2	Kapsamlı inceleme ve analiz çalışmaları sonucuyla ilgili bildirimleri ilgili birimlere yapar.
				D.5.3	Yapılan çalışmanın raporunu hazırlar.

Görevler		**İşlemler**		**Başarım Ölçütleri**	
Kod	**Adı**	**Kod**	**Adı**	**Kod**	**Açıklama**
E	Siber güvenlik risk analizi ve yönetimi çalışmalarına katılmak	**E.1**	Siber güvenlik analizlerinde kullanılan sistemlerin çalışma ve sürdürülebilirliğini takip etmek	**E.1.1**	Siber güvenlik analizlerinde kullanılan sistemler üzerinde incelenen tüm kaynaklardan gerekli verilerin alındığının kontrolünü yapar.
				E.1.2	Siber güvenlik analizlerinde kullanılan sistem kaynaklarının kullanım oranlarını takip eder.
				E.1.3	Siber güvenlik analizlerinde kullanılan sistemlerin üzerinde oluşturulan alarm kurallarını inceleyerek düzenler.
				E.1.4	Efektif çalışmasına yönelik düzenli çalışmalar gerçekleştirir.
				E.1.5	Güncel tehditler ve yaşanılan güvenlik olaylarını göz önünde bulundurarak sistem üzerinde yeni alarm kuralları oluşturur.
		E.2	İleri düzey 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.
				E.2.5	Kurumun bilgi güvenliği risk analiz ve yönetimi süreçlerine katılarak destek verir.

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 mesleki gelişim sağlayacak etkinlikleri takip eder.
				F.1.2	Kariyer hedeflerine yönelik eğitimler, çalışmalar ve faaliyetlere katılarak mesleki gelişimini oluşturur.
				F.1.3	Uluslararası Siber Güvenlik Standartlarını ve ilgili mesleki gruplarını takip eder.
		F.2	Takım arkadaşlarının mesleki gelişimini desteklemek	**F.2.1**	Bilgi ve deneyimlerini takım arkadaşları ile paylaşır.
				F.2.2	Yeni elemanların yetişmeleri ve yetkin olmalarına iş süreçleri kapsamında destek verir.

3.2. Kullanılan Araç, Gereç ve Ekipman

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

3.3. Bilgi ve Beceriler

1. Acil durum talimatları
2. Acil durum talimatlarının iş süreçlerinde uygulanması
3. Adli bilişim süreci hakkında bilgi
4. Ağ teknolojileri bilgisi
5. Ağ ve güvenlik cihazları hakkında bilgi
6. Alarm kuralları hakkında bilgi
7. Analitik düşünme becerisi
8. Bilgi güvenliği risk analiz ve yönetimi süreçleri hakkında bilgi
9. Bilgi güvenliği yönetim sistemi standartları ve uygulama teknikleri bilgisi
10. Bilgi sistemleri envanteri oluşturma bilgi ve becerisi
11. Bilgi sistemleri kaynakları hakkında bilgi
12. Bilgisayar donanımları ve çevre birimleri bilgisi
13. Bilişim altyapısının siber güvenlik ihtiyaçlarını belirleme becerisi
14. Bilişim altyapısının siber güvenlik ihtiyaçlarını hakkında bilgi
15. Çalışma için gerekli yazılım, donanım ve ekipmanları çalışmaya hazır hale getirme becerisi
16. Çevre koruma talimatları
17. Çevre koruma talimatlarının iş süreçlerinde uygulanması
18. Çevre koruma yöntemleri ve yasal düzenlemeler bilgisi
19. Çevresel tehlike ve riskler ile bunlara karşı alınacak önlemler hakkında bilgi
20. Çevresel tehlike ve risklere karşı alınan önlemleri uygulama becerisi
21. Dijital arşivleme işlemleri hakkında bilgi

22. Dijital arşivleme yapma becerisi
23. Ekip yönetimi becerisi
24. Faaliyetler için temin edilecek yazılım, donanım ve ekipman hakkında bilgi
25. Güvenli ağ ve internet bağlantısı kurulum bilgisi ve uygulama becerisi
26. Güvenlik donanım araç ve gereçleri bilgisi
27. Güvenlik teknolojileri temel kullanım bilgisi ve uygulama becerisi
28. Güvenlik testleri hakkında bilgi
29. İSG talimatları hakkında bilgi
30. İSG talimatlarının iş süreçlerinde uygulanması
31. İş organizasyonu ve planlama becerisi
32. İş planı yapma işlemleri hakkında bilgi ve beceri
33. İş süreçlerinde ortaya çıkan atıklar hakkında bilgi
34. İş süreçlerinde uygulanması gereken kalite şartları/gereklilikleri hakkında bilgi
35. İş süreçlerinin kalite şartları/gerekliliklerine göre gerçekleştirilmesi işlemleri hakkında bilgi ve beceri
36. İşlemler esnasında kullanılacak kişisel koruyucu donanımlar hakkında bilgi ve bunların kullanım becerisi
37. İşletim sistemi ve uygulama iz kayıtları hakkında bilgi
38. İşletim sistemleri ve servisler hakkında bilgi
39. İşletim sistemleri ve sunucu yazılımları bilgisi
40. İz kayıtlarını inceleme ve yorumlama becerisi
41. Kimlik ve kaynak yönetimi bilgisi
42. Kriz yönetimi bilgi ve becerisi
43. Kullanılan araç, gereç ve ekipmanlar hakkında bilgi ve bunların işlemlere hazır hale getirilmesi becerisi
44. Kullanılan sistemin çalışma ve sürdürülebilirliğini takip etme bilgi ve becerisi
45. Mesleğe ilişkin yasal düzenlemeler bilgisi
46. Mesleki matematik, terim ve yabancı dil bilgisi
47. Ortaya çıkan atıkların tasnifi ve bertarafına yönelik işlemler hakkında bilgi ve beceri
48. Programlama bilgisi
49. Risk yönetimi bilgi ve becerisi
50. Risk, tehlike ve ramak kala olaylara karşı yapılacak işlemler hakkında bilgi ve işlemlerin uygulanması becerisi
51. Sağlık ve güvenlik işaretleri ve talimatları hakkında bilgi
52. Sektöre ait ulusal ve uluslararası standartlar bilgisi
53. Siber güvenlik analizlerinde kullanılacak sistemler hakkında bilgi
54. Siber güvenlik analizlerinde kullanılacak sistemlerin çalışma ve sürdürülebilirliğini takip etme becerisi
55. Siber güvenlik farkındalığı oluşturma işlemleri hakkında bilgi ve beceri
56. Siber güvenlik risk analizi ve yönetiminde görev ve sorumlulukları hakkında bilgi ve beceri
57. Siber olay için aksiyon belirleme bilgi ve becerisi
58. Siber olay için alınan aksiyonu takip etme becerisi
59. Siber olay kaynaklarını hakkında bilgi
60. Siber olay kaynaklarını inceleme becerisi
61. Siber olay yönetim organizasyonu hakkında bilgi
62. Siber olay yönetim organizasyonunu gerçekleştirme becerisi

63. Sistem kaynakları hakkında bilgi
64. Sistem ve uygulama yazılımları bilgisi
65. Şifreleme ve algoritma bilgisi
66. Tehlike, risk ve ramak kala olaylar hakkında bilgi
67. Teknik dokümanları okuma ve anlama bilgi ve becerisi
68. Temel çalışma mevzuatı bilgisi
69. Temel iş sağlığı ve güvenliği bilgisi
70. Terminoloji ve atak vektörleri hakkında bilgi
71. Terminoloji ve atak vektörleri hakkında güncelleme yapma becerisi
72. Veri tabanı güvenliği bilgi ve becerisi
73. Veri toplama, kayıt tutma ve raporlama bilgi ve becerisi
74. Yangın önleme, yangınla mücadele, acil durum ve tahliye bilgisi
75. Yapılan işlemler esnasında ortaya çıkan kayıtlar hakkında bilgi
76. Yapılan işlemler ile ilgili kayıtlara yönelik yapacağı işlemler hakkında bilgi ve beceri
77. Yazılı ve sözlü iletişim becerisi
78. Zafiyet yönetimi hakkında bilgi
79. Zafiyet yönetimi yapma bilgi ve becerisi
80. Zaman yönetimi becerisi
81. Zararlı yazılımlar hakkında bilgi

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. Bilgi akışında bilinmesi gerekenler prensibine göre hareket etmek
5. Çalışma zamanını iş emrine uygun şekilde etkili ve verimli kullanmak
6. Çevre, kalite ve İSG mevzuatında yer alan düzenlemeleri benimsemek
7. Çevreyi korumaya karşı duyarlı olmak
8. Deneyimlerini iş arkadaşlarına aktarmak
9. Doğal kaynakların etkin kullanmak
10. Görev gereği edinilen kişisel veya hassas verilerin gizliliğine riayet etmek
11. İşletme kaynaklarının kullanımı ve geri kazanım konusunda duyarlı olmak
12. İşyeri çalışma prensiplerine uymak
13. İşyeri hiyerarşi ilişkisine uygun hareket etmek
14. İşyeri prosedür ve talimatlarına uygun davranmak
15. Kendisinin ve diğer kişilerin güvenliğini gözetmek
16. Mesleki gelişim için araştırmaya istekli olmak
17. Risk değerlendirmesinde belirtilen hususlar ile İSG kurallarına riayet etmek
18. Risk faktörleri konusunda duyarlı olmak
19. Sorumluluklarını zamanında yerine getirmek
20. Tehlike durumlarında ilgilileri zamanında bilgilendirmek
21. Temizlik, düzen ve işyeri tertibine özen göstermek
22. Vardiya değişimlerinde etkili, açık ve doğru şekilde bilgi paylaşmak
23. 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.

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 ORUK	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

Doç. Dr. Ahmet ÖZMEN	Üye (Yükseköğretim Kurulu Başkanlığı)
Harun DEMİR	Üye (Sanayi ve Teknoloji Bakanlığı)
Ömer Faruk YILDIRIM	Üye (Milli Eğitim Bakanlığı)
Mesut AKANER	Üye (Aile, Çalışma ve Sosyal Hizmetler Bakanlığı)
Muzaffer ÇALIŞKAN	Üye (Ulaştırma ve Altyapı Bakanlığı)
Melek BAR ELMAS	Üye (Türkiye Odalar ve Borsalar Birliği)
Muhammet Şükrü KÜÇÜK	Üye (Hak İşçi Sendikaları Konfederasyonu)
Tayfun ARIKAZAN	Üye (Türkiye İşveren Sendikaları Konfederasyonu)
Umut CÜYAZ	Üye (Türkiye Esnaf ve Sanatkârları Konfederasyonu)
Dilek TORUN	Üye (Mesleki Yeterlilik Kurumu)

Yaprak AKÇAY ZİLELİ	Daire Başkanı, Mesleki Yeterlilik Kurumu
Esma DOĞAN	Uzman Yardımcısı, Mesleki Yeterlilik Kurumu

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