SİBER GÜVENLİK ELEMANI

SEVİYE 5

REVİZYON NO: 00

23UY0544-5

GİRİŞ

Siber Güvenlik Elemanı (Seviye 5) Ulusal Yeterliliği 19/10/2015 tarihli ve 29507 sayılı Resmi Gazete'de yayımlanan Ulusal Meslek Standartlarının ve Ulusal Yeterliliklerin Hazırlanması Hakkında Yönetmelik ve 27/11/2007 tarihli ve 26713 sayılı Resmi 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.

TERİMLER, SİMGELER VE KISALTMALAR

ACİL DURUM: İşyerinin tamamında veya bir kısmında meydana gelebilecek veya işyerini dışarıdan etkileyebilecek yangın, patlama, tehlikeli kimyasal maddelerden kaynaklanan yayılım, zehirlenme, salgın hastalık, radyoaktif sızıntı, sabotaj ve doğal afet gibi ivedilikle müdahale gerektiren olayları,

ACİL DURUM PLANI: İşyerlerinde meydana gelebilecek acil durumlarda yapılacak iş ve işlemler ile uygulamaya yönelik eylemlerin yer aldığı planı

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: 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,

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

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,

SOME: Siber Olaylara Müdahale Ekibini,

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,
USOM: Ulusal Siber Olaylara Müdahale Merkezini,
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.

23UY0544-5 SİBER GÜVENLİK ELEMANI ULUSAL YETERLİLİĞİ

1	**YETERLİLİĞİN ADI**	Siber Güvenlik Elemanı
2	**REFERANS KODU**	23UY0544-5
3	**SEVİYE**	5
4	**ULUSLARARASI SINIFLANDIRMADAKİ YERİ**	ISCO 08: 2529 (Başka yerde sınıflandırılmamış veri tabanı ve bilgisayar ağları ile ilgili profesyonel meslek mensupları)
5	**TÜR**	
6	**KREDİ DEĞERİ**	
7	**A) YAYIN TARİHİ**	01/02/2023
	B) REVİZYON NO	00
	C) REVİZYON TARİHİ	
8	**AMAÇ**	Siber Güvenlik Elemanı (Seviye 5) mesleğinin eğitim almış ve nitelik kazandırılmış kişiler tarafından yürütülmesi ve çalışmalarda kalitenin artırılması için; • Adayların sahip olması gereken nitelikleri, bilgi, beceri ve yetkinlikleri tanımlamak, • Adayların, geçerli ve güvenilir bir belge ile mesleki yeterliliğini kanıtlamasına olanak vermek, • Eğitim sistemine, sınav ve belgelendirme kuruluşlarına referans ve kaynak oluşturmak amacıyla hazırlanmıştır.
9	**YETERLİLİĞE KAYNAK TEŞKİL EDEN MESLEK STANDART(LAR)I**	
19UMS0740-5 – Siber Güvenlik Elemanı (Seviye 5) Ulusal Meslek Standardı		
10	**YETERLİLİK SINAVINA GİRİŞ ŞART(LAR)I**	
-		
11	**YETERLİLİĞİN YAPISI**	
11-a) Zorunlu Birimler		
23UY0544-5/A1 İş Sağlığı ve Güvenliği, Çevre Koruma ve Kalite Gereklilikleri 23UY0544-5/A2 Siber Güvenlik Çalışmalarının Yürütülmesi		
11-b) Seçmeli Birimler		
-		
11-c) Birimlerin Gruplandırılma Alternatifleri		
Adayın yeterlilik belgesi alabilmesi için zorunlu yeterlilik birimlerin tamamından başarılı olması gerekmektedir.		
12	**ÖLÇME VE DEĞERLENDİRME**	
Mesleki Yeterlilik Belgesini elde etmek isteyen adaylar birimlerde tanımlanan sınavlara tabi tutulur. Yeterlilik birimlerindeki teorik ve performansa dayalı sınavları her bir birim için ayrı ayrı yapılabileceği gibi birlikte de yapılabilir. Ancak her birimin değerlendirmesi bağımsız yapılmalıdır. Yeterlilik birimlerinin geçerlilik süresi, birimin başarıldığı tarihten itibaren 2 yıldır. Yeterlilik birimlerinin birleştirilerek bir yeterliliğin elde edilebilmesi için tüm birimlerin geçerliliğini koruyor		

olması gerekmektedir.		
13	**DEĞERLENDİRİCİ ÖLÇÜTLERİ**	
Değerlendiricilerin aşağıdaki ölçütlerden en az birini sağlıyor olması gerekmektedir: • Siber güvenlik konularında en az üç (3) yıl öğretmen/öğretim üyesi/öğretim görevlisi olarak üniversitelerde veya meslek liselerinde eğitim vermiş olmak, • Mühendislik fakülteleri (Bilgisayar, Bilişim Sistemleri, Elektrik Elektronik, Yazılım, Endüstri Mühendisliği) programlarından mezun olmak ve siber güvenlik alanında en az beş (5) yıl deneyime sahip olmak, • Lisans mezunu olmak ve siber güvenlik alanında en az yedi (7) yıl deneyime sahip olmak. Yukarıdaki özelliklerden en az birine sahip olan ve ölçme ve değerlendirme sürecinde görev alacak değerlendiricilere; sınav ve belgelendirme kuruluşları tarafından mesleki yeterlilik sistemi, kişinin görev alacağı ulusal yeterlilik(ler), ilgili uluslararası/ulusal meslek standart(lar)ı, ölçme-değerlendirme, ölçme-değerlendirmede kalite güvencesi ve İSG konularında eğitim sağlanmalıdır.		
14	**BELGE GEÇERLİLİK SÜRESİ**	Belgenin geçerlilik süresi beş (5) yıldır.
15	**GÖZETİM SIKLIĞI**	-
16	**BELGE YENİLEMEDE UYGULANACAK ÖLÇME-DEĞERLENDİRME YÖNTEMİ**	5 yıllık geçerlilik süresinin sonunda belge sahibinin performansı, aşağıda tanımlanan yöntemlerden en az biri kullanılarak değerlendirmeye tabi tutulur; a) 5 yıl belge geçerlilik süresi içerisinde toplamda en az iki yıl veya son altı ay boyunca ilgili alanda çalıştığını gösteren kayıtları (hizmet dökümü, referans yazısı/mektubu, sözleşme, fatura, portfolyo, vb.) sunmak, b) Yeterlilik kapsamında yer alan yeterlilik birimleri için tanımlanan Uygulama (Performans) Sınavından (P1) başarılı olmak Bu şartlardan en az birini yerine getiren adayların belge geçerlilik süreleri 5 yıl daha uzatılır.
17	**MESLEKTE YATAY ve DİKEY İLERLEME YOLLARI**	Yatay ilerleme: Etik Hacker (Seviye 5)
18	**YETERLİLİĞİ GELİŞTİREN KURULUŞ(LAR)**	Bilgi Teknolojileri ve İletişim Kurumu
19	**YETERLİLİĞİ DOĞRULAYAN SEKTÖR KOMİTESİ**	MYK Bilişim Teknolojileri Sektör Komitesi

23UY0544-5/A1 İŞ SAĞLIĞI VE GÜVENLİĞİ, ÇEVRE KORUMA VE KALİTE GEREKLİLİKLERİ YETERLİLİK BİRİMİ

1	**YETERLİLİK BİRİMİ ADI**	İş Sağlığı ve Güvenliği, Çevre Koruma ve Kalite Gereklilikleri
2	**REFERANS KODU**	23UY0544-5
3	**SEVİYE**	5
4	**KREDİ DEĞERİ**	
5	**A) YAYIN TARİHİ**	01/02/2023
	B) REVİZYON NO	00
	C) REVİZYON TARİHİ	
6	**YETERLİLİK BİRİMİNE KAYNAK TEŞKİL EDEN MESLEK STANDARDI**	
19UMS0740-5 – Siber Güvenlik Elemanı (Seviye 5) Ulusal Meslek Standardı		
7	**ÖĞRENME KAZANIMLARI**	

Öğrenme Kazanımı 1: İş sağlığı ve güvenliği önlemlerini açıklar.

Alt Öğrenme Kazanımları:
1.1: İş sağlığı ve güvenliği ile ilgili uygulaması gereken önlemleri açıklar.
1.2: Acil durum prosedürlerini açıklar.

Öğrenme Kazanımı 2: Çevre koruma ve kalite gerekliliklerini açıklar.

Alt Öğrenme Kazanımları:
2.1: Çevre koruma ile ilgili uygulaması gereken önlemleri açıklar.
2.2: İş süreçlerinde uygulaması gereken kalite gerekliliklerini açıklar.

8	**ÖLÇME VE DEĞERLENDİRME**

8 a) Teorik Sınav

(T1): A1 birimine yönelik teorik sınav Ek A1-2'de yer alan "Bilgiler" kontrol listesine göre gerçekleştirilir. Teorik sınavda adaylara 4 seçenekli çoktan seçmeli ve her biri eşit puan değerinde en az 16 soruluk sınav uygulanmalıdır.
Sınavda yanlış cevaplandırılan sorulardan herhangi bir puan indirimi yapılmaz, adaylara her soru için bir buçuk (1,5) dakika zaman verilir. Teorik sınavda sorulardan en az %70'ine doğru yanıt veren aday başarılı sayılır. Sınav soruları bu birimde teorik sınav ile ölçülmesi öngörülen tüm bilgi ifadelerini (Ek A1-2) ölçmelidir.

8 b) Performansa Dayalı Sınav

A1 birimine yönelik beceri ve yetkinlik ifadeleri, diğer birimlerin beceri ve yetkinlik kontrol listelerinde tanımlanmış olup, bu kapsamda ölçme ve değerlendirmesi yapılacaktır.

8 c) Ölçme ve Değerlendirmeye İlişkin Diğer Koşullar

Yeterlilik biriminin geçerlilik süresi birimin başarıldığı tarihten itibaren 2 yıldır.

9	**YETERLİLİK BİRİMİNİ GELİŞTİREN KURUM/KURULUŞ(LAR)**	Bilgi Teknolojileri ve İletişim Kurumu
10	**YETERLİLİK BİRİMİNİ DOĞRULAYAN SEKTÖR KOMİTESİ**	MYK Bilişim Teknolojileri Sektör Komitesi

YETERLİLİK BİRİMİ EKLERİ

EK [A1]-1: Yeterlilik Biriminin Kazandırılması için Tavsiye Edilen Eğitime İlişkin Bilgiler

1. **İş sağlığı ve güvenliğine yönelik temel düzenlemeler**
   1.1. İş sağlığı ve güvenliğinde işverenlerin ve çalışanların hukuki yükümlülükleri
   1.2. Araç, gereç ve ekipmanların güvenli kullanımı ile ilgili talimat ve prosedürler ve bunları iş süreçlerine uygulama
   1.3. Çalışma ortamı ve yapılan işten kaynaklı tehlike ve riskler
   1.4. Risk ve tehlike kavramları, türleri ve özellikleri
   1.5. Risk değerlendirmesi ve ramak kala olay kavramları
   1.6. İş kazası ve ramak kala durumlarında uygulanacak prosedürler
   1.7. KKD kullanımı
   1.8. Çalışma ortamında güvenli çalışma için uyulması gereken önlemler
   1.9. Çalışma ortamında bulunabilecek sağlık ve güvenlik işaretleri ve donanımları
   1.10. Acil durum kapsamı ve acil durum planı
   1.11. Acil durum türleri ve acil durumlarda harekât tarzı
   1.12. Acil durumda uyulması gereken kurallar
   1.13. Çalışma alanının iş sağlığı ve güvenliği açısından kontrolü
2. **Çevresel risklerin azaltılmasına yönelik uygulamalar**
   2.1. Çalışma süreçlerinde ortaya çıkan atık malzemelerin tasnif ve bertarafı
   2.2. Çalışma süreçlerinde ortaya çıkan elektronik atıkların tasnif ve bertarafı
   2.3. Temel atık yönetimi
   2.4. Üretim süreçlerinde meydana gelmesi olası çevresel risk ve tehlikeler
   2.5. Çevresel risk ve tehlikelere karşı uygulaması gereken önlemler
   2.6. Enerji verimliliği ve temel tasarruf uygulamaları
3. **İş süreçlerinde kalite gereklilikleri, iş organizasyonu ve mesleki gelişim ile ilgili faaliyetler**
   3.1. Süreçlerle ilgili takip edilmesi gereken mevzuatlar
   3.2. Çalışma süreçlerinde kalitenin sağlanmasına yönelik izlenmesi gereken prosedürler
   3.3. Tutulması gereken kayıtlar ve raporlama
   3.4. Temel kalite yönetim süreçleri
   3.5. Çalışma süreçlerinde karşılaşılması olası hatalar ve bunların giderilmesi süreci

EK [A1]-2: Yeterlilik Biriminin Ölçme ve Değerlendirmesinde Kullanılacak Kontrol Listesi

a) BİLGİLER

No	Bilgi İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı

No	Bilgi İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BG.1	İş sağlığı ve güvenliği ile ilgili terimleri (tehlike, risk, risk değerlendirmesi ve ramak kala olay) ayırt eder.	A.1.1	1.1	T1
BG.2	Çalışma süreçlerindeki koşullara göre temel İSG tehlike ve risklerini belirler.	A.1.1	1.1	T1
BG.3	Üretim süreçlerindeki olası İSG tehlike ve risklerine göre uygulaması gereken önlemleri açıklar.	A.1.4	1.1	T1
BG.4	Siber güvenlik ile ilgili süreçlerde kullanması gereken KKD'leri ayırt eder.	A.1.3	1.1	T1
BG.5	Çalışma ortamında bulunabilecek güvenlik donanımlarını ve bunlara ilişkin talimatları açıklar.	A.1.2	1.1	T1
BG.6	Çalışma ortamında bulunabilecek sağlık ve güvenlik işaretlerini ve bunlara ilişkin talimatları açıklar.	A.1.6	1.1	T1
BG.7	Acil durum kapsamını ve acil durum planını açıklar.	A.2.1	1.2	T1
BG.8	Acil durumlarda uyulması gereken kuralları ve yapılması gerekenleri açıklar.	A.2.2	1.2	T1
BG.9	İş süreçlerinde ortaya çıkan atık malzemelerin (kablolar ve benzeri) tasnif ve bertarafına yönelik prosedürleri açıklar.	A.3.2	2.1	T1
BG.10	İş süreçlerinde ortaya çıkan elektronik atıkların tasnif ve bertarafına yönelik prosedürleri açıklar.	A.3.2	2.1	T1
BG.11	Üretim süreçlerinde meydana gelmesi olası çevresel risk ve tehlikeleri açıklar.	A.3.1 A.3.2	2.1	T1
BG.12	Çevresel risk ve tehlikelere karşı uygulaması gereken önlemleri sıralar.	A.3.1 A.3.2	2.1	T1
BG.13	İş süreçlerinde kalitenin sağlanmasına yönelik izlemesi gereken prosedürleri açıklar.	A.4.2	2.2	T1
BG.14	İş süreçlerinde tutması gereken kayıtları ve raporlaması gereken işlemleri sıralar.	A.4.2	2.2	T1
BG.15	İş süreçlerinde karşılaşılması olası hataları sıralar.	A.4.1	2.2	T1
BG.16	Hataların giderilmesine yönelik yöntemleri açıklar.	A.4.1	2.2	T1

b) BECERİ VE YETKİNLİKLER

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
*BY.1	-	-	-	-

(*) Performans sınavında başarılması zorunlu kritik adımlar.

23UY0544-5/A2 SİBER GÜVENLİK ÇALIŞMALARININ YÜRÜTÜLMESİ YETERLİLİK BİRİMİ

1	**YETERLİLİK BİRİMİ ADI**	Siber Güvenlik Çalışmalarının Yürütülmesi
2	**REFERANS KODU**	23UY0544-5
3	**SEVİYE**	5
4	**KREDİ DEĞERİ**	
5	**A) YAYIN TARİHİ**	01/02/2023
	B) REVİZYON NO	00
	C) REVİZYON TARİHİ	
6	**YETERLİLİK BİRİMİNE KAYNAK TEŞKİL EDEN MESLEK STANDARDI**	
19UMS0740-5 – Siber Güvenlik Elemanı (Seviye 5) Ulusal Meslek Standardı		
7	**ÖĞRENME KAZANIMLARI**	

Öğrenme Kazanımı 1: Çalışma süreçlerinde sistemlerin işlevselliğini ve güvenliğini sağlar.

Alt Öğrenme Kazanımları:
1.1: Çalışma sürecinde İSG ve çevre koruma önlemlerini uygular.
1.2: Kalite ve bilgi güvenliği prosedürlerini uygular.

Öğrenme Kazanımı 2: İş organizasyonunu yapar.

Alt Öğrenme Kazanımları:
2.1: İş planlamasını yapar.
2.2: Faaliyetler için yazılım, donanım ve ekipman temin eder.
2.3: Yapılan işlerin kaydını tutar.
2.4: Dijital arşivleme yapar.

Öğrenme Kazanımı 3: Siber güvenlik önleyici faaliyet çalışmalarına katılır.

3.1: Bilgi sistemleri envanteri oluşturur.
3.2: Zafiyet takibi yapar.
3.3: Siber güvenlik farkındalığı oluşturma yöntemlerini açıklar.

Öğrenme Kazanımı 4: Siber olay yönetim sürecine katılır.

4.1: Terminoloji ve atak vektörleri hakkında güncellemeleri takip eder.
4.2: Siber olay kaynaklarını inceler.
4.3: Olay değerlendirmesi yapar.
4.4: Siber olay için aksiyon belirler.
4.5: Aksiyon takibi yapar.

Öğrenme Kazanımı 5: Siber güvenlik risk analizi ve yönetimi çalışmalarına katılır.

5.1: Siber güvenlik analizlerinde kullanılan sistemlerin çalışma ve sürdürülebilirliğini takip eder.
5.2: İleri düzey inceleme ve analiz çalışmalarına destek verir.

8	ÖLÇME VE DEĞERLENDİRME

8 a) Teorik Sınav

(T1): A2 birimine yönelik teorik sınav Ek A2-2'de yer alan "Bilgiler" kontrol listesine göre gerçekleştirilir. Teorik sınavda adaylara 4 seçenekli çoktan seçmeli ve her biri eşit puan değerinde en az 15 soruluk sınav uygulanmalıdır. Sınavda yanlış cevaplandırılan sorulardan herhangi bir puan indirimi yapılmaz, adaylara her soru için 1,5 dakika zaman verilir. Teorik sınavda sorulardan en az %70'ine doğru yanıt veren aday başarılı sayılır. Sınav soruları bu birimde teorik sınav ile ölçülmesi öngörülen tüm bilgi ifadelerini (Ek A2-2) ölçmelidir.

8 b) Performansa Dayalı Sınav

(P1): A2 birimine yönelik performansa dayalı sınav Ek A2- 2'de yer alan "Beceriler ve Yetkinlikler" kontrol listesine göre gerçekleştirilir. Beceri ve yetkinlikler kontrol listesinde aday tarafından başarılması zorunlu kritik adımlar belirlenir. Adayın, performans sınavından başarı sağlaması için kritik adımların tamamından başarılı performans göstermek koşuluyla sınavın genelinden asgari %70 başarı göstermesi gerekir. Performansa dayalı sınavın süresi gerçek uygulama şartlarındaki süreye karşılık gelmelidir.

Performansa dayalı sınav gerçek veya gerçeğine uygun olarak düzenlenmiş laboratuvar ortamında gerçekleştirilir. Beceri ve yetkinlik ifadelerinin (Ek A2-2) tamamı performansa dayalı sınav ile ölçülmelidir.

8 c) Ölçme ve Değerlendirmeye İlişkin Diğer Koşullar

Birim için öngörülen sınavların geçerlilik süresi sınavın başarıldığı tarihten itibaren 1 yıldır. Birimin elde edilebilmesi için başarılan sınav tarihleri arasındaki süre farkı 1 yılı geçemez. Birimin elde edilebilmesi için adayların birimde tanımlanan tüm sınavlardan başarılı olması gerekir.

Yeterlilik biriminin geçerlilik süresi birimin başarıldığı tarihten itibaren 2 yıldır.

Adayın kendi ve diğer kişilerin can güvenliğini tehlikeye sokacak bir davranış göstermesi halinde adayın sınavına son verilir.

9	YETERLİLİK BİRİMİNİ GELİŞTİREN KURUM/KURULUŞ(LAR)	Bilgi Teknolojileri ve İletişim Kurumu
10	YETERLİLİK BİRİMİNİ DOĞRULAYAN SEKTÖR KOMİTESİ	MYK Bilişim Teknolojileri Sektör Komitesi

YETERLİLİK BİRİMİ EKLERİ

EK [A2]-1: Yeterlilik Biriminin Kazandırılması için Tavsiye Edilen Eğitime İlişkin Bilgiler

1. **Üretim süreçlerinde sistemlerin işlevselliğini ve güvenliği**
   1.1. Çalışma sürecinde İSG ve çevre önlemleri
   1.2. Kalite ve bilgi güvenliği prosedürleri

2. **İş organizasyonunu yapma**
   2.1. İş planlaması
   2.2. Faaliyetler için yazılım, donanım ve ekipman temini
   2.3. Kayıt tutma
   2.4. Dijital arşivleme

3. **Siber güvenlik önleyici faaliyet çalışmaları**
   3.1. Bilgi sistemleri envanteri oluşturma
   3.2. Zafiyet ve olayların takibi
   3.3. Gerçekleştirilen güvenlik testleri sonuçlarını inceleme
   3.4. Siber güvenlik farkındalığı oluşturma

4. **Siber olay yönetim sürecine katılma**
   4.1. Terminoloji ve atak vektörleri
   4.2. Siber olay kaynakları
   4.3. Bilgi sistemleri kaynaklarının güncel durumunun kontrolü
   4.4. Gerçekleşen olayların kategorizasyonu
   4.5. İz kayıtlarından rapor ve alarm oluşturma
   4.6. Olay değerlendirmesi yapma ve siber olay tespiti
   4.7. Siber olay için aksiyon belirleme
   4.8. Aksiyon formu doldurma
   4.9. Aksiyon takibi yapma

5. **Siber güvenlik risk analizi ve yönetimi çalışmalarına katılma**
   5.1. Siber güvenlik analizlerinde kullanılan sistemlerin çalışma ve sürdürülebilirliği
   5.2. İleri düzey inceleme ve analiz çalışmaları
   5.3. Mesleki gelişimle ilgili, ulusal ve uluslararası siber güvenlik grupları (USOM, SOME), kurumları ve sertifikaları

EK [A2]-2: Yeterlilik Biriminin Ölçme ve Değerlendirmesinde Kullanılacak Kontrol Listesi

a) BİLGİLER

No	Bilgi İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BG.1	Siber güvenlik işlemlerinde kullanılacak donanım ve yazılım gibi ekipmanları tanımlar.	B.2.1-2	2.1	T1
BG.2	Bilgi sistemleri envanteri oluşturulması için gerekli işlemleri açıklar.	C.1.1-4	3.1	T1
BG.3	Zafiyet takibini ile ilgili gerekli işlemleri açıklar.	C.2.1-5	3.2	T1
BG.4	Siber güvenlik farkındalığı oluşturma yöntemlerini açıklar.	C.3.1-5	3.3	T1
BG.5	Terminoloji ve güncel atak vektörlerini tanımlar.	D.1.1-3	4.1	T1
BG.6	Terminoloji ve atak vektörleri hakkında güncellemeleri takip eder.	D.1.1-3	4.1	T1
BG.7	Olası siber olay kapsamında bilişim sistemlerinde gerekli izleme ve ilişkilendirme işlemlerini tanımlar.	D.2.1-4	4.2	T1
BG.8	Gerçekleşen olayları (kötücül yazılım, veri sızıntısı ve benzeri) kategorize eder.	D.3.7	4.3	T1
BG.9	Olası siber olay için belirlenebilecek aksiyonları tanımlar.	D.4.1-3	4.4	T1
BG.10	Siber güvenlik analizinde kullanılan sistemlerin çalışma ve sürdürebilirliği konusunda gerekli kontrolleri açıklar.	E.1.1-5	5.1	T1

No	Bilgi İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BG.11	İleri düzey siber güvenlik inceleme ve analiz çalışmalarını konusunda gerekli kontrolleri açıklar.	E.2.1-5	5.2	T1
BG.12	Mesleki gelişimle ilgili, ulusal ve uluslararası siber güvenlik grupları (USOM, SOME), kurumları ve sertifikaları açıklar.	F.1.1-3	5.2	T1

b) BECERİ VE YETKİNLİKLER

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
*BY.1	Çalışmaları sırasında İSG kurallarına ve talimatlarına uygun şekilde hareket eder.	A.1.1-6 A.2.1-2	1.1	P1
*BY.2	Çalışmaları sırasında çevre koruma talimatlarına uygun şekilde hareket eder.	A.3.1-2	1.1	P1
*BY.3	Çalışmaları sırasında kalite talimatlarına uygun şekilde hareket eder.	A.4.1-2	1.2	P1
BY.4	İşletme yöntem, kural ve formatlarına uygun olarak iş emirlerini sistemden/ilgili birimden/amirden alarak gelen iş emrine yönelik ilgili kaynaklardan bilgi toplar.	B.1.1	2.1	P1
BY.5	Aldığı iş emirlerine ve topladığı bilgilere göre yapılacak faaliyetlerin sınıflamasını ve sıralamasını yaparak tahmini işlem sürelerini saptar.	B.1.2	2.1	P1
*BY.6	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.1.4	2.1	P1
BY.7	İş süreçlerinde kullanacağı ekipman ve yazılımların ön kontrollerini yapar.	B.2.1	2.2	P1
*BY.8	Çalışma için gerekli yazılım, donanım ve ekipmanı çalışmaya hazır hale getirir.	B.2.2	2.2	P1
*BY.9	İş emri, süreç, fire/hata, ölçüm gibi formları işletme formatlarına uygun olarak doldurur.	B.3.1	2.3	P1
BY.10	Amirin kontrol ve onayı sonrasında, formları ilgili birimlere iletir.	B.3.4	2.3	P1
*BY.11	İş süreçleri sonunda oluşan rapor, form ve benzeri kaynak materyallerin sonraki düzeylerde teknik aktarım amacıyla işletme kural ve yöntemlerine uygun olarak arşivlenmesini sağlar.	B.4.2	2.4	P1
BY.12	Dijital arşivin güvenlik ve koruma önlemlerini işletme kural ve yöntemlerine göre uygular.	B.4.3	2.4	P1

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
*BY.13	Kullanılan ağ ve güvenlik cihazları, uygulamalar, işletim sistemleri, servisler ve diğer bilişim alt yapısına yönelik sistemler hakkında bilgi toplayarak topladığı bilgileri raporlar.	C.1.1-2	3.1	P1
*BY.14	Kullanılan bilgi sistemleri envanterini oluşturarak raporlar.	C.1.3-4	3.1	P1
*BY.15	Kullanılan bilgi sistemlerinde çıkan zafiyet ve olayları takip eder.	C.2.1	3.2	P1
*BY.16	Gerçekleştirilen güvenlik testleri sonuçlarını inceleyerek ilgili kişilere iletir.	C.2.2-3	3.2	P1
BY.17	Bilgi sistemleri kaynaklarının güncel durumunu (erişilebilirliğini ve yükünü) kontrol ederek raporlar.	D.2.1-2	4.2	P1
*BY.18	Bilgi sistemleri kaynaklarından gerekli iz kayıtlarının siber güvenlik analizi için kullanılan sistemlerde toplanmasında ve iz kayıtlarının ilişkilendirilip zenginleştirilmesinde görev alır.	D.2.3-4	4.2	P1
*BY.19	İlişkilendirilen iz kayıtlarından rapor ve alarm oluşturur.	D.3.1	4.3	P1
*BY.20	Oluşan alarm ve iz kayıtlarını inceleyerek siber olayı tespit eder.	D.3.2-3	4.3	P1
BY.21	İncelemeler doğrultusunda olay bildirimi oluşturur.	D.3.4	4.3	P1
BY.22	Yapılan bildiri ve iletilen bilgiler ile ilgili aksiyon formunu doldurur.	D.4.3	4.4	P1
BY.23	Alınması gereken aksiyonlar ile ilgili süreçlerin takibini gerçekleştirir.	D.4.3	4.5	P1
*BY.24	Siber güvenlik analizlerinde kullanılan sistemler üzerinde incelenen tüm kaynaklardan gerekli verilerin alındığının kontrolünü yapar.	E.1.1	5.1	P1
BY.25	Siber güvenlik analizlerinde kullanılan sistem kaynaklarının kullanım oranlarını takip eder.	E.1.2	5.1	P1
*BY.26	Siber güvenlik analizlerinde kullanılan sistemlerin üzerinde oluşturulan alarm kurallarını inceleyerek düzenler.	E.1.3	5.1	P1
*BY.27	Güncel tehditler ve yaşanılan güvenlik olaylarını göz önünde bulundurarak sistem üzerinde yeni alarm kuralları oluşturur.	E.1.5	5.1	P1
BY.28	Güvenlik testi çalışmalarında kapsam belirleme, gerekli izinlerin tanımlanması, sistemlerin işleyişi ve çalışmanın sağlıklı devam edebilmesi için gerekli kontrollerin yapılması konularında katkı vererek sonuçları raporlar.	E.2.2	5.2	P1
BY.29	Zararlı yazılım analizi süreçlerine; zararlı yazılımın tespiti, bulunması, muhafaza edilmesi, iletilmesi ve karşı aksiyonların alınması konularında katkı verir.	E.2.3	5.2	P1

No	Beceri ve Yetkinlik İfadesi	UMS İlgili Bölüm	Yeterlilik Birimi Alt Öğrenme Kazanımı	Değerlendirme Aracı
BY.30	Adli bilişim sürecini yöneten ekibe; imaj alma, verinin saklanması, iletilmesi ve oluşturulacak zaman çizelgesi hazırlanması konularında katkı verir.	E.2.4	5.2	P1

(*) Performans sınavında başarılması zorunlu kritik adımlar.

YETERLİLİK EKLERİ

EK 1: Ulusal Yeterlilik Hazırlama Ekibi ve Teknik Çalışma Grubu Üyeleri

	Adı - Soyadı	**Eğitim Bilgileri* (Tarih - Eğitim Kurumu/Bölüm Adı)**	**Deneyim Bilgileri* (Tarih – İş Yeri – Unvan)**
1.	Yakup Hakan COŞKUN (Moderatör)	2004 - Hacettepe Üniversitesi Kamu Yönetimi Bölümü	• 2016-Devam ediyor Pamir Uygunluk Değerlendirme Ltd.Şti. • 2008-2015 Mesleki Yeterlilik Kurumu • 2005-2008 İŞKUR
2.	Onur AKTAŞ	Daire Başkanı	Bilgi Teknolojileri ve İletişim Kurumu
3.	Emre MÜLAZIMOĞLU	Mühendis	Bilgi Teknolojileri ve İletişim Kurumu
4.	Mustafa Kaan İLTER	Mühendis	Bilgi Teknolojileri ve İletişim Kurumu
5.	Fatih ÖZKUL	Mühendis	Bilgi Teknolojileri ve İletişim Kurumu

**Yalnızca meslekle ilgili olan eğitim/deneyim bilgilerine yer verilecektir.*

EK 2: Görüş İstenen Kişi, Kurum ve Kuruluşlar

Çalışma ve Sosyal Güvenlik Bakanlığı (İş Sağlığı ve Güvenliği Genel Müdürlüğü)
Ankara Sanayi Odası (ASO)
Ankara Ticaret Odası (ATO)
ASELSAN
Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Yüksek Lisans Programı
Bilgi Güvenliği Derneği
Bilişim Teknolojileri ve Siber Güvenlik Derneği
Ege Bölgesi Sanayi Odası (EBSO)
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
Hak-İş Konfederasyonu
HAVELSAN
Işık Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Yüksek Lisans Programı
İç İşleri Bakanlığı (Emniyet Genel Müdürlüğü)
İstanbul Şehir Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı
İstanbul Teknik Üniversitesi Bilişim Enstitüsü Bilişim Uygulamaları Anabilim Dalı Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programı
İstanbul Ticaret Odası (İTO)
İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Anabilim Dalı

Kadir Has Üniversitesi Siber Güvenlik ve Kritik Altyapı Koruma Uygulama ve Araştırma Merkezi
Kamu Siber Güvenlik Derneği
Küçük ve Orta Ölçekli İşletmeleri Geliştirme ve Destekleme İdaresi Başkanlığı
MEB Hayat Boyu Öğrenme Genel Müdürlüğü
MEB Mesleki ve Teknik Eğitim Genel Müdürlüğü
MEB Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü
Milli Savunma Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı Siber Güvenlik Yüksek Lisans Programı
NETAŞ
Ortadoğu Teknik Üniversitesi Enformatik Enstitüsü Siber Güvenlik Anabilim Dalı
Sabancı Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi Siber Güvenlik Lisansüstü Programı
STM
Süleyman Demirel Üniversitesi Mühendislik Mimarlık Fakültesi Uzaktan Eğitim Bilgisayar Mühendisliği Siber Güvenlik Tezsiz Yüksek Lisans
TOBB ETÜ Fen Bilimleri Enstitüsü Siber Güvenlik Lisans Üstü Programı
TURKCELL
TÜRK TELEKOM
Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
Türkiye Bilişim Derneği
Türkiye Esnaf ve Sanatkârları Konfederasyonu (TESK)
Türkiye İhracatçılar Meclisi (TİM)
Türkiye İstatistik Kurumu (TÜİK)
Türkiye İş Kurumu (İş ve Meslek Danışmanlığı Dairesi Başkanlığı)
Türkiye İşçi Sendikaları Konfederasyonu (TURK-İŞ)
Türkiye İşveren Sendikaları Konfederasyonu (TİSK)
Türkiye Odalar ve Borsalar Birliği (TOBB)
Uluslararası Siber Güvenlik Federasyonu
VODAFONE
Yükseköğretim Kurulu Başkanlığı (YÖK)

EK 3: MYK Sektör Komitesi Üyeleri ve Uzmanlar

Prof. Dr. Ahmet ÖZMEN	Başkan (Yükseköğretim Kurulu Başkanlığı)
Yasemin AKPINAR	Başkan Vekili (Milli Eğitim Bakanlığı)
Mesut AKANER	Üye (Çalışma ve Sosyal Güvenlik Bakanlığı)
Sümeyye İSLAMOĞLU	Üye (Sanayi ve Teknoloji Bakanlığı)
İsrafil Bilge TAŞDEMİR	Üye (Ulaştırma ve Altyapı Bakanlığı)
Ertan BARUT	Üye (Türkiye Odalar ve Borsalar Birliği)
Uğur GÖKDERE	Üye (Türkiye İşveren Sendikaları Konfederasyonu)
Umut Barış ERDOĞAN	Üye (Türkiye İşçi Sendikaları Konfederasyonu)
Umut CÜYAZ	Üye (Türkiye Esnaf ve Sanatkârları Konfederasyonu)
Esma DOĞAN	Üye (Mesleki Yeterlilik Kurumu)
Yaprak AKÇAY ZİLELİ	Daire Başkanı, Mesleki Yeterlilik Kurumu

EK 4: MYK Yönetim Kurulu Üyeleri

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