*Bu form, İşletmede Mesleki Eğitimini tamamlayan Ege Üniversitesi Siber Güvenlik Meslek Yüksekokulu öğrencisinin performansının ölçülmesi ve başarı notunun belirlenmesi amacıyla hazırlanmıştır.*

|  |  |
| --- | --- |
| Yetkilinin Adı Soyadı /  Unvanı |  |
| İşletmenin Adı ve  Faaliyet Alanı |  |
| Öğrencinin Adı Soyadı |  |
| İşyeri Uygulama Tarihleri | Başlama: ……../……./….. Bitiş: ……../……./….. |

*Öğrencimizin, kişisel ve mesleki niteliklerini aşağıda verilen Tablo 1’deki puanlama cetvelini kullanarak İşletmede Mesleki Eğitim kapsamında değerlendiriniz.* ***“Mesleki bilgi, yeteneği ve işlerde başarı derecesi****” için Mesleki Yeterlilik Kurumu’nun Siber Güvenlik Elemanı Mesleki Yeterlilik Kriterleri temel alınarak hazırlanan Tablo 2’ye uygun olarak puanlama yapılacaktır. Yapılan puanlamaya göre %10’u alınarak hesaplamaya dahil edilecektir.*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Tablo 1: Puanlama Cetveli** | | | | | | | | | | | | | |  |
| **ÖĞRENCİNİN** | | | | | | **Çok iyi** | **İyi** | | **Orta** | **Yetersiz** | | **Çok Yetersiz** | |  |
| 1. **Mesleki bilgisi, yeteneği, işlerde başarı derecesi\*** | | | | | | *Tablo 2’ye göre yapılan değerlendirme sonucu verilen puanın %10’u alınacaktır.* | | | | | | | |
| 1. Verilen işi algılama, zamanında ve tam yapma, uygulayabilme yeteneği ve isteği | | | | | |  |  | |  |  | |  | |
| 1. Ekip çalışmasına uyumu, iletişim becerileri | | | | | |  |  | |  |  | |  | |
| 1. Görev ve sorumluluk bilinci, özverili çalışma | | | | | |  |  | |  |  | |  | |
| 1. İş disiplini, işe devam durumu | | | | | |  |  | |  |  | |  | |
| 1. İş güvenliği kurallarına uyumu | | | | | |  |  | |  |  | |  | |
| 1. Çalışanlara karşı tutumu ve çevresi ile sosyal uyumu | | | | | |  |  | |  |  | |  | |
| 1. Kendine güveni ve ifade etme yeteneği | | | | | |  |  | |  |  | |  | |
| 1. İnisiyatif alma, öneri getirme, eleştirel düşünebilme yeteneği | | | | | |  |  | |  |  | |  | |
| 1. İşletmede Mesleki Eğitim süresi içerisinde mesleki gelişimi | | | | | |  |  | |  |  | |  | |
| **İşletmede Mesleki Eğitim İşyeri Genel Değerlendirme Sonucu** Başarılı Başarısız | | | | | | | | | | | | | |
| Genel olarak öğrencimizi, aşağıdaki puanlama cetveline göre, işyerinde geçirmiş olduğu uygulama  eğitimi kapsamında nasıl değerlendirirsiniz? (Puanlar 100’lük sisteme göre aralık olarak verilmiştir.) | | | | | | | | | | | | | | |
| 89-100 |  | 74-80 |  | 60-66 |  | | | 46- 52 |  | |  | |  | |
| 81-87 |  | 67-73 |  | 53-59 |  | | | 0 - 46 |  | |  | |  | |

**Değerlendirme Kriterlerinin Tanımları:**

**Risk Değerlendirme ve Raporlama:** Çalışma ortamındaki tehlikeleri gözlemleme, risk değerlendirme çalışmalarına katılma ve sonuçları ilgili birimlere raporlama.

**Ekipman ve Yazılım Kullanımı:** Çalışma için gerekli yazılım, donanım ve ekipmanların doğru kullanımını ve çalışır durumda olmasını sağlama.

**Siber Güvenlik Zafiyetlerini Tespit Etme:** Zafiyet tarama araçlarını kullanarak açıkları belirleme ve raporlama.

**Bilgi Güvenliği Farkındalığı Oluşturma:** Güvenlik politikalarına uygun içerikler hazırlama ve farkındalık artırıcı bilgilendirmeler yapma.

**Siber Olay İnceleme ve Raporlama**: Olay kayıtlarını inceleme, analiz etme, gerektiğinde olayları kategorize ederek ilgili aksiyonları başlatma.

**Veri ve Kayıtların Doğru Yönetimi:** Çalışma sürecinde oluşan veri ve kayıtları eksiksiz ve doğru bir şekilde tutma, dijital arşivleme süreçlerini etkin şekilde uygulama.

**Kalite ve Verimlilik Çalışmalarına Katkı Sağlama:** İş süreçlerinde hataları tespit etme, kalite standartlarına uygun iyileştirme önerileri geliştirme.

**Siber Tehdit Analizi ve Raporlama:** Tehdit istihbaratı araçlarını kullanarak mevcut tehditleri analiz etme ve ilgili birimlere raporlama.

**Siber Güvenlik Risk Yönetimi:** Risk analizi yaparak sistem açıklarını değerlendirme, önleyici tedbirleri planlama ve uygulama.

**Siber Güvenlik İyileştirme Önerileri Geliştirme:** Mevcut güvenlik sistemlerini analiz ederek, yeni tehditlere karşı çözüm ve iyileştirme önerileri geliştirme.

**Dereceli Değerlendirme Tablosu**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kriterler** | **1. Düzey (Geliştirilmeli)** | **2. Düzey (Orta Düzeyde Başarılı)** | **3. Düzey (Üstün Başarılı)** | **Puan** |
| **1. Risk Değerlendirme ve Raporlama** | Riskler eksik gözlemlenmiş, raporlama yapılmamış. | Riskler gözlemlenmiş, temel düzeyde raporlama yapılmış. | Riskler detaylı analiz edilmiş, etkili bir rapor hazırlanmış. |  |
| **2. Ekipman ve Yazılım Kullanımı** | Ekipman ve yazılımlar hatalı veya yetersiz şekilde kullanılmış. | Ekipmanlar ve yazılımlar doğru ancak sınırlı bir kapasitede kullanılmış. | Ekipmanlar etkin ve doğru şekilde, tam kapasiteyle kullanılmış. |  |
| **3. Siber Güvenlik Zafiyetlerini Tespit Etme** | Zafiyet tarama araçları kullanılmamış veya yanlış uygulanmış. | Zafiyet taramaları yapılmış ancak sonuçlar eksik analiz edilmiş. | Zafiyetler tam olarak tespit edilmiş, detaylı raporlama yapılmış. |  |
| **4. Bilgi Güvenliği Farkındalığı Oluşturma** | İçerikler hazırlanmamış veya farkındalık artırıcı çalışmalar yapılmamış. | Temel farkındalık materyalleri hazırlanmış, etkinlikler sınırlı kalmış. | Etkili materyaller hazırlanmış, farkındalık düzeyi önemli ölçüde artırılmış. |  |
| **5. Siber Olay İnceleme ve Raporlama** | Olay kayıtları incelenmemiş, analiz yapılmamış. | Olaylar temel düzeyde incelenmiş ancak eksiklikler mevcut. | Olaylar detaylı analiz edilmiş ve sonuçlar doğru bir şekilde raporlanmış. |  |
| **6. Veri ve Kayıtların Doğru Yönetimi** | Veriler eksik tutulmuş veya yanlış arşivlenmiş. | Veriler temel düzeyde arşivlenmiş ancak doğruluk eksik. | Veriler eksiksiz, doğru şekilde yönetilmiş ve arşivlenmiş. |  |
| **7. Kalite ve Verimlilik Çalışmalarına Katkı Sağlama** | Hatalar tespit edilmemiş veya kalite standartları uygulanmamış. | Temel düzeyde iyileştirme önerileri geliştirilmiş. | Süreçlerde kalite standartları uygulanmış, etkili öneriler sunulmuş. |  |
| **8. Siber Tehdit Analizi ve Raporlama** | Tehdit analizi araçları kullanılmamış veya sonuçlar hatalı raporlanmış. | Temel tehdit analizleri yapılmış, ancak eksiklikler mevcut. | Tehditler detaylı analiz edilmiş ve stratejik rapor hazırlanmış. |  |
| **9. Siber Güvenlik Risk Yönetimi** | Risk analizi yapılmamış veya önlemler uygulanmamış. | Risk analizi yapılmış, ancak önlemler kısmen uygulanmış. | Risk analizi eksiksiz yapılmış, önlemler etkin şekilde uygulanmış. |  |
| **10. Siber Güvenlik İyileştirme Önerileri Geliştirme** | Mevcut sistemler analiz edilmemiş, iyileştirme önerileri sunulmamış. | Temel düzeyde öneriler geliştirilmiş, ancak eksiklikler var. | Sistemler detaylı analiz edilmiş, kapsamlı ve etkili öneriler sunulmuş. |  |

**Puanlama Açıklamaları**

**10 puan (3. düzey)**: Performans kriterin gerekliliklerini karşılamıyor. Geliştirme ve tekrar değerlendirme önerilir.

**6 puan (2. düzey)**: Performans kısmen yeterli; belirli eksikliklerin giderilmesi gerekiyor.

**3 puan (1. düzey)**: Performans kriterin gerekliliklerini karşılamıyor. Geliştirme ve tekrar değerlendirme önerilir.