	HAKKARİ ÜNİVERSİTESİ **GÖREV TANIMI FORMU**

BİRİMİ	:	Bilgi İşlem Daire Başkanlığı
GÖREV ADI	:	Siber Olaylara Müdahale Ekibi
AMİRİ	:	Bilgi İşlem Daire Başkanı
SORUMLULUK ALANI	:	Üniversite bilişim altyapısı, ağ, sistem, uygulama ve servislerinde meydana gelebilecek siber olayların önlenmesi, tespiti, müdahalesi ve iyileştirilmesi. "7545 sayılı Siber Güvenlik Kanunu", "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", "5809 sayılı Elektronik Haberleşme Kanunu", "6698 sayılı Kişisel Verilerin Korunması Kanunu", "5237 sayılı Türk Ceza Kanunu" ve ilgili diğer mevzuat hükümleri çerçevesinde görev yapmak. "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" ve "Ulusal Siber Güvenlik Stratejileri ve Eylem Planları" kapsamında yükümlülükleri yerine getirmek. Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve gerektiğinde Sektörel Siber Olaylara Müdahale Ekipleri ile koordinasyon sağlamak.
YERİNE GÖREVLENDİRİLECEK KİŞİ	:	Daire Başkanı tarafından uygun görülen, bilgi güvenliği, ağ yönetimi, sistem yönetimi ve yazılım alanlarında yetkin personeller.
GÖREV AMACI	:	Hakkari Üniversitesi bilişim sistemlerini hedef alan siber tehditleri önlemek, gerçekleşen olaylara etkin şekilde müdahale etmek, bilgi güvenliği ihlallerini en aza indirmek, ulusal siber güvenlik ekosistemiyle uyumlu bir müdahale ve koordinasyon mekanizması yürütmek.
TEMEL İŞ VE SORUMLULUKLAR	:	1- Siber tehditleri izleme ve tespit etme Üniversite bilgi sistemlerine yönelik anormal trafik, saldırı girişimleri ve güvenlik açıklarını tespit etmek. Açık kaynak istihbarat, Ulusal Siber Olaylara Müdahale Merkezi (USOM) bildirimleri, uluslararası güvenlik uyarıları ve kurum içi tehdit istihbaratı prosedürü çerçevesinde düzenli siber tehdit izleme faaliyetleri yürütmek. 2- Olay müdahalesi gerçekleştirme Tespit edilen siber olaylara hızla müdahale ederek etkilerini en aza indirmek, sistemleri güvenli hâle getirmek. Olaylara ilişkin delilleri (log kayıtları, trafik verileri) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve ilgili diğer mevzuat hükümlerine uygun şekilde toplamak, saklamak ve gerektiğinde adli mercilere sunmak.

		3- Koordinasyon sağlama Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ kapsamında, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve gerekli görülen durumlarda Sektörel Siber Olaylara Müdahale Ekipleri ile koordinasyonu sağlamak. Kurum içi birimler, dış paydaşlar ve ilgili otoriteler ile etkin iletişim kurmak. 4- Zafiyet yönetimi Bilgi sistemlerinde tespit edilen güvenlik açıklarını değerlendirmek ve kapatılması için ilgili birimleri yönlendirmek. Güncel siber tehditler ve yazılım/hardware üreticilerinin güvenlik yamaları doğrultusunda sistemlerin sürekli güncel tutulmasını sağlamak. 5- Kök neden analizi yapmak Meydana gelen siber olayların nedenlerini inceleyerek tekrarını önleyici teknik ve idari tedbirler belirlemek. "7545 sayılı Siber Güvenlik Kanunu" ve Ulusal Siber Güvenlik Stratejileri çerçevesinde, kurum içi prosedürleri gözden geçirip risk temelli iyileştirmeler önermek. 6- Kayıt ve raporlama Tüm siber olay kayıtlarını tutmak, periyodik ve olay sonrası raporlar hazırlayarak üst yönetime sunmak. 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında, kişisel veri ihlallerini tespit etmesi halinde gerekli bildirimleri yerine getirmek. USOM ve yetkili kamu otoritelerine yapılması gereken zorunlu raporlamaları süresinde gerçekleştirmek. 7- Siber güvenlik farkındalığı oluşturmak Personel ve öğrencilere yönelik güvenlik farkındalığı eğitimleri düzenlemek, bilgilendirme çalışmaları yapmak. Phishing simülasyonları ve bilinçlendirme faaliyetleri ile kullanıcıların farkındalık seviyesini ölçmek ve artırmak. 8- Sürekli iyileştirme SOME iş süreçlerini, teknik altyapıyı ve prosedürleri düzenli olarak gözden geçirip geliştirmek. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, ISO/IEC 27035 Bilgi Güvenliği Olay Yönetimi Standardı, NIST Siber Güvenlik Çerçevesi ve Avrupa Birliği Siber Güvenlik

		Ajansı (ENISA) Rehberleri doğrultusunda uyum çalışmaları yürütmek.
YETKİLERİ	:	1- Üniversite birimlerinden SOME faaliyetleri kapsamında gerekli her türlü bilgi, belge, kayıt ve logları talep etme ve inceleme yetkisine sahiptir. 2- Olay müdahalesi sırasında ilgili bilgi sistemlerine erişim, konfigürasyon değişikliği ve müdahale yapma yetkisi. 3- Üniversite bilgi sistemlerini siber güvenlik açısından inceleme, güvenlik testleri yapma ve zafiyet taraması gerçekleştirme yetkisi. 4- Meydana gelen siber olaylar, güvenlik açıkları ve müdahale sonuçları hakkında üst yönetim ve USOM'a düzenli rapor sunma yetkisi. 5- USOM, diğer kurum SOME'leri ve ilgili ulusal/uluslararası paydaşlarla iş birliği ve koordinasyon sağlama yetkisi. 6- Siber güvenlik risklerini azaltmaya yönelik teknik, idari ve organizasyonel önlemleri önermek ve acil durumlarda uygulamak. 7- Üniversite personeline ve öğrencilere yönelik siber güvenlik farkındalık eğitimleri planlama ve düzenleme yetkisi.

GÖREV TANIMINI HAZIRLAYAN		
ADI SOYADI: Bahar OĞUR	TARİH: 06.01.2025	İMZA:
ONAYLAYAN		
ADI SOYADI: Ümmü Gülsüm ÜMİT	TARİH: 06.01.2025	İMZA:

Bu dokümanda açıklanan görev tanımımı okudum. Görevimi burada belirtilen kapsamda yerine getirmeyi kabul ediyorum.

KOMİSYON ÜYELERİ

Adı Soyadı:	Gülşen ERTUŞ	**Adı Soyadı:**	Ömer ÇİÇEK	**Adı Soyadı:**	Diyar ÇAKAR
Unvan:	Öğretim Görevlisi	**Unvan:**	Mühendis	**Unvan:**	Büro Personeli
Tarih:	06.01.2025	**Tarih:**	06.01.2025	**Tarih:**	06.01.2025
İmza:		**İmza:**		**İmza:**	