***Ek-10.1:*** *12.11.2024/09-10 gün ve sayılı Senato kararı ekidir.*



**YILDIZ TEKNİK ÜNİVERSİTESİ**

**SİBER GÜVENLİK KOORDİNATÖRLÜĞÜ KURULUŞ VE ÇALIŞMA YÖNERGESİ**

**BİRİNCİ BÖLÜM**

**Amaç, Kapsam, Dayanak ve Tanımlar**

(12.11.2024 günlü 2024/09-10 sayılı Senato kararı ile yürürlüğe girmiştir.)

**Amaç**

**MADDE 1-** (1) Bu yönergenin amacı, Üniversitenin bilgi sistemleri, ağ altyapısı, dijital varlıkları ve kişisel verilerin korunmasını sağlamak ve siber tehditlere karşı alınacak tedbirleri düzenlemekle görevli Yıldız Teknik Üniversitesi Siber Güvenlik Koordinatörlüğü’nün çalışma usul ve esaslarını belirlemektir.

**Kapsam**

**MADDE 2-** (1) Bu yönerge “Yıldız Teknik Üniversitesi Siber Güvenlik Koordinatörlüğü” nün çalışma usul ve esaslarını kapsar.

**Dayanak**

**MADDE 3-** (1)Bu yönerge; 2547 Sayılı Yükseköğretim Kanunu’nun 14. Maddesine dayanılarak hazırlanmıştır.

**Tanımlar**

**MADDE 4-** (1)Bu yönergede geçen;

1. Başkanlık: Yıldız Teknik Üniversitesi Bilgi İşlem Daire Başkanlığını,
2. Kişisel Veri: 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında kimliği belirli veya belirlenebilir gerçek kişilere ilişkin her türlü bilgiyi,
3. Koordinatör: Yıldız Teknik Üniversitesi Siber Güvenlik Koordinatörünü,
4. Koordinatörlük: Yıldız Teknik Üniversitesi Siber Güvenlik Koordinatörlüğünü,
5. Kurul: Yıldız Teknik Üniversitesi Siber Güvenlik Kurulunu,
6. Rektör: Yıldız Teknik Üniversitesi Rektörünü,
7. Sızma Testi: Sistemlerin ve ağların güvenlik açıklarını tespit etmek amacıyla yapılan güvenlik testlerini,
8. Siber Güvenlik Uzmanı: Sistem güvenliği, ağ güvenliği, zararlı yazılım analizi, veri güvenliği, sızma testi ve diğer güvenlik operasyonlarından sorumlu uzman personeli,
9. Siber Olay: Bilgi sistemlerinin işleyişine zarar verebilecek, yetkisiz erişim, veri hırsızlığı veya dijital varlıkların bütünlüğünü tehlikeye atabilecek olayları,
10. Siber Olaylara Müdahale Ekibi (SOME): Üniversite bünyesinde siber olaylara müdahale amacıyla oluşturulan ekibi,
11. Üniversite: Yıldız Teknik Üniversitesini,
12. Senato: Yıldız Teknik Üniversitesi Senatosunu,
13. Zararlı Yazılım: Bilgi sistemlerine zarar vermek amacıyla geliştirilen her türlü yazılım veya kodları ifade eder.

**İKİNCİ BÖLÜM**

**Koordinatörlüğün Görevleri**

**Görevleri**

**MADDE 5-** (1) Koordinatörlüğün görevleri şunlardır:

1. Üniversitenin, bilgi güvenliği strateji ve politikasını, güncel tehditler ve gelişen teknolojilere uygun olarak güncellemek.
2. Üniversitenin ağ altyapısı, sunucu sistemleri, veri tabanları ve dijital varlıklarının güvenliğini sağlamak için gerekli güvenlik önlemlerini almak.
3. Üniversitenin bilgi sistemlerini hedef alabilecek olası siber saldırıları tespit etmek, önlemek ve gerekli önlemleri almak.
4. Üniversitenin bilgi sistemlerine yönelik düzenli olarak sızma testleri yaparak güvenlik açıklarını tespit etmek ve gidermek.
5. Bilgi sistemlerinde zararlı yazılım taramaları yapmak ve tespit edilen yazılımları temizlemek.
6. Üniversitenin kişisel veri işleme süreçleri ile ilgili tedbirleri almak ve kontrol etmek.
7. Üniversitenin siber saldırılara karşı acil müdahale planlarını hazırlamak ve olası saldırı durumlarında müdahale etmek.
8. ğ) Üniversite personeli ve öğrencilerine yönelik düzenli olarak siber güvenlik farkındalık eğitimleri düzenlemek ve güvenlik bilincini artırmak.
9. Üniversitenin bilişim sistemlerine yönelik gerçekleşen tüm siber olay ve saldırıların sistematik takibini yapmak, bunlarla ilgili kayıtları tutmak, tutulan kayıtları belgelendirmek ve raporlamak.
10. Yukarıda belirtilen görevlerle ilgili olarak düzenlenen raporları ilgili birim ve kurumlara standart formatlar kullanarak bildirmek.

**ÜÇÜNCÜ BÖLÜM**

**Organlar ve Görevleri**

**Organlar**

**MADDE 6-** (1)Siber Güvenlik Koordinatörlüğünün organları şunlardır:

1. Siber Güvenlik Kurulu
2. Koordinatör
3. Koordinatör Yardımcısı

**Siber Güvenlik Kurulu Oluşumu**

**MADDE 7-** (1)Siber Güvenlik Kurulu Eğitim-Öğretim Rektör Yardımcısı’nın başkanlığında Bilgi İşlem Daire Başkanı, Koordinatör ile siber güvenlik alanında uzman personel arasından Rektör tarafından görevlendirilecek iki (2) kişi olmak üzere toplam beş (5) kişiden oluşur.

(2) Kurul altı (6) ayda bir toplanır. Bunun dışında gerekli görülmesi halinde Eğitim-Öğretim Rektör Yardımcısı’nın çağrısı ile toplanabilir.

(3) Kurul üye tam sayısının salt çoğunluğu ile toplanır. Üye tam sayısının salt çoğunluğu ile karar alır.

(4) Kurul üyelerinin görev süresi dört (4) yıldır. Görev süresi dolan üye yeniden görevlendirilebilir.

**Görevleri**

**MADDE 8-** (1) Kurulun görevi,Üniversitenin bilgi güvenliğine ilişkin strateji ve politikasını belirlemek ve uygulanmasını sağlamaktır.

**Koordinatör**

**MADDE 9-** (1) Koordinatör, siber güvenlik alanında uzman olan personel arasından Rektör tarafından dört (4) yıl süre ile görevlendirilir. Süresi biten koordinatör yeniden görevlendirilebilir.

(2) Herhangi bir nedenle görev süresi dolmadan koordinatörlük görevinin sona ermesi durumunda aynı usulle yeniden koordinatör görevlendirilir.

(3) Koordinatöre çalışmalarında yardımcı olmak üzere, koordinatörün önerisi ve Rektörün onayı ile bir (1) koordinatör yardımcısı görevlendirilebilir.

**Koordinatörün Görevleri**

**MADDE 10-** (1) Sorumlu olduğu koordinatörlüğü sevk ve idare etmek, koordinatörlük iş ve işlemlerini, kurumun amaç ve hedefleri doğrultusunda ekonomik, kaliteli, etkin ve verimli bir şekilde gerçekleştirmeye yönelik organizasyon ve iş planlaması yapmak, uygulamaları denetlemek, Koordinatörlüğün kuruluş amacı ve felsefesi doğrultusunda faaliyette bulunmak,

1. Kurum içi ve kurum dışında Koordinatörlüğü temsil etmek,
2. Koordinatörlük çalışanları arasında eşgüdümü sağlamak, görev, yetki ve sorumluklarını belirlemek,
3. Koordinatörlüğün her türlü ihtiyaçlarını belirlemek ve karşılanmasını sağlamak,
4. Koordinatörlüğün her türlü taşınır mal işlemlerinin kontrolünü yapmak,
5. Koordinatörlüğün faaliyet raporlarını ve istatiksel raporlarını hazırlamak ve üst yönetime sunmak,
6. Birim internet sitesinin kullanım amacına uygun ve güncel olmasını sağlamak,
7. Verilecek benzeri görevleri yürütmek.

**DÖRDÜNCÜ BÖLÜM**

**Siber Olaylara Müdahale Ekibi (SOME), Müdahale**

**Siber Olaylara Müdahale Ekibi (SOME)**

**MADDE 11-** (1)Koordinatörlük bünyesinde, siber güvenlik uzmanları istihdam edilebilir. İhtiyaç duyulması halinde, Koordinatör tarafından Siber Olaylara Müdahale Ekibi (SOME) oluşturulabilir.

(2) Siber güvenlik uzmanları ile Siber Olaylara Müdahale Ekibinin (SOME) görevleri Üniversitenin ağ ve sistem güvenliğini sağlamak, zararlı yazılım analizi yapmak, zararlı yazılımlara ilişkin temizleme işlemlerini yapmak, bilgi sistemlerinde tespit edilen güvenlik açıklarını gidermek, düzenli olarak güvenlik testleri ve izlemelerini yapmaktır.

**Müdahale**

**MADDE 12 –** (1) Üniversite bilişim sistemlerine yönelik gerçekleşen siber saldırı, veri ihlali veya güvenlik zafiyetleri durumunda Koordinatörlük tarafından, acil müdahale planlarının devreye sokulması ve müdahale edilmesi gerekir.

**BEŞİNCİ BÖLÜM**

**Çeşitli Hükümler**

**MADDE 13 –** (1)Üniversiteninsiber güvenlik strateji ve politikalarının yürütülmesi ve teknik altyapı kararlarının alınması ve uygulanmasında Koordinatörlük ve Başkanlık ortak karar almak ve birlikte çalışmak zorundadır.

(2) Koordinatörlüğün giderleri Başkanlık bütçesinden karşılanır.

**ALTINCI BÖLÜM**

**Yürürlük ve Yürütme**

**Yürürlük**

**MADDE 14-** (1)Bu yönerge, Senato tarafından onaylandığı tarihte yürürlüğe girer.

**Yürütme**

**MADDE 15-** (1) Bu yönerge hükümleri Rektör tarafından yürütür.