SİVAS CUMHURİYET ÜNİVERSİTESİ
NANOFOTONİK UYGULAMA VE ARAŞTIRMA MERKEZİ (CÜNAM)

CÜNAM DİJİTAL ALTYAPI VE UZAKTAN ERİŞİM GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

MADDE 1 – Amaç

(1) Bu Yönergenin amacı, CÜNAM'ın yönettiği dijital sistemler ile kurum dışından erişilebilen uygulamaların güvenli kullanımını ve sunucu, lisanslı yazılım, kiosk ve cihaz bilgisayarlarına erişim esaslarını belirlemektir.

MADDE 2 – Kapsam

(1) Bu Yönerge, CÜNAM personelini ve CÜNAM bünyesinde çalışan öğrencileri; LYS kullanan kurum dışı kişileri ve teknik destek sağlayıcılarını ilgili işlemleri bakımından kapsar. CÜNAM sunucusu ve sanal makineleri, lisanslı yazılımlar, LYS, kiosklar, cihaz bilgisayarları ve kurumsal dijital süreç platformu bu Yönergenin kapsamındadır.

(2) İnternet ağı, sunucu IP tahsisi ve kurumsal e-posta hizmetleri üniversitenin Bilgi İşlem birimi üzerinden sağlanır. CÜNAM'ın kendi sistemlerine ilişkin görevleri, üniversitenin bu hizmetlerdeki yetkileriyle koordineli olarak yürütülür. Üniversite tarafından sağlanan internet erişimine ilişkin erişim kayıtlarının tutulması Üniversitenin, CÜNAM'ın kendi sunucu, uygulama ve ağ altyapısına ilişkin kayıtların tutulması CÜNAM'ın sorumluluğundadır; bu paylaşım Yönetim Kurulu kararı ve protokol ile belirlenir.

MADDE 3 – Dayanak

(1) Bu Yönerge, 6550 sayılı Araştırma Altyapılarının Desteklenmesine Dair Kanun ile ilgili uygulama yönetmeliğinin araştırma altyapılarının yönetimi, güvenliği ve kullanımına ilişkin hükümleri; 6698 sayılı Kişisel Verilerin Korunması Kanunu, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 7545 sayılı Siber Güvenlik Kanunu, İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik ve ilgili diğer mevzuat dikkate alınarak hazırlanmıştır.

MADDE 4 – Tanımlar

(1) Bu Yönergede CÜNAM, Sivas Cumhuriyet Üniversitesi Nanofotonik Uygulama ve Araştırma Merkezini; Yönetim Kurulu, CÜNAM Yönetim Kurulunu; Müdür, CÜNAM müdürünü; Müdür Yardımcısı, CÜNAM müdür yardımcısını; LYS, laboratuvar ve cihaz rezervasyon sistemini ifade eder.

(2) Kurumsal dijital süreç platformu, CÜNAM'ın iş ve kayıt süreçlerinde kullandığı elektronik sistemi; CÜNAM Bilgi İşlem birimi, merkezin bilgi işlem görevlerini yürüten personeli ifade eder.

SİVAS CUMHURİYET ÜNİVERSİTESİ
NANOFOTONİK UYGULAMA VE ARAŞTIRMA MERKEZİ (CÜNAM)

İKİNCİ BÖLÜM

Yönetim ve Erişim Yetkileri

MADDE 5 – Görev ve sorumluluklar

(1) Yönetim Kurulu, bu Yönergeyi ve önemli istisnaları onaylar; temel kaynak ve risk önceliklerini belirler. Müdür uygulamayı koordine eder, sistem sahiplerini görevlendirir ve kritik olaylarda karar alır. Müdür Yardımcısı, Müdürün kendisine verdiği görevleri yürütür.

(2) CÜNAM Bilgi İşlem birimi, merkezin yönettiği bilişim sistemlerinin teknik işletimini yürütür. Program sorumluları lisanslı yazılımlara erişecek kişileri, cihaz sorumluları ise cihaz bilgisayarlarının kullanım ihtiyacını belirler; teknik konularda CÜNAM Bilgi İşlem birimi ile koordinasyon kurarlar.

(3) Kullanıcı kendisine verilen erişim bilgilerini korur, yalnızca yetkili olduğu sistem ve kayıtlara erişir; şüpheli bir durumu CÜNAM Bilgi İşlem birimine bildirir.

MADDE 6 – Dijital sistemlerin takibi

(1) CÜNAM'ın yönettiği sunucu, sanal makineler, uygulamalar, kiosklar ve cihaz bilgisayarlarının teknik sorumluları ile kullanım amaçları takip edilir. Sistemlerin erişim ve yedekleme kapsamı ayrı ayrı değerlendirilir.

MADDE 7 – Hesap ve erişim yetkileri

(1) Kurum dışı kullanıcı LYS'ye kayıt olduğunda hesabı doğrudan açılır; cihaz rezervasyonunun onayı ayrı bir işlemdir. CÜNAM personeli ve CÜNAM bünyesinde çalışan öğrencilerin kurumsal dijital süreç platformu hesapları CÜNAM Bilgi İşlem birimince tanımlanır. Kayıt sırasında kullanıcıya 6698 sayılı Kanunun 10 uncu maddesi uyarınca aydınlatma metni sunulur.

(2) CÜNAM ile çalışma ilişkisi sona eren personel ve öğrencilerin kurumsal dijital süreç platformu hesapları CÜNAM Bilgi İşlem birimince kapatılır.

MADDE 8 – Kimlik doğrulama ve oturum güvenliği

(1) LYS'ye kullanıcı adı veya e-posta adresi ve şifre ile giriş yapılır. Kurum dışından da erişilebilen kurumsal dijital süreç platformunda iki aşamalı doğrulama bütün kullanıcılar için zorunludur. Kullanıcılar kendilerine ait hesap bilgilerini başkalarına veremez.

(2) Ortak kullanılan lisanslı program şifresinin yetkisiz kişiye geçtiğinden şüphelenilirse program sorumlusu CÜNAM Bilgi İşlem birimiyle iletişime geçer ve yeni şifre oluşturulur. Kullanılmayan oturumlar kapatılır veya kilitlenir.

SİVAS CUMHURİYET ÜNİVERSİTESİ
NANOFOTONİK UYGULAMA VE ARAŞTIRMA MERKEZİ (CÜNAM)

ÜÇÜNCÜ BÖLÜM

Kurum Dışından Erişim ve Teknik Sistemler

MADDE 9 – Kurum dışından erişimin sınırları

(1) LYS'ye kurum dışından kayıtlı kullanıcılar erişebilir; kurumsal dijital süreç platformuna ise yalnızca yetkili CÜNAM personeli ve CÜNAM bünyesinde çalışan öğrenciler erişebilir. Sunucu üzerindeki lisanslı programlara erişim, CÜNAM kurum ağına bağlı yetkili iç kullanıcılarla sınırlıdır; bu programlara kurum dışından kullanıcı bağlantısı verilmez.

(2) Üretici veya servis sağlayıcının uzaktan teknik destek bağlantısı yalnızca ilgili bakım veya arıza işlemi için açılır ve CÜNAM personeli tarafından takip edilir. İşlem sonunda bağlantı kapatılır; firmaya sürekli erişim tanımlanmaz. Teknik destek yerinde de verilebilir.

MADDE 10 – Kurumsal dijital süreç platformu

(1) Platform kullanıcısı kendi projesi için ayrı bir kayıt açabilir. Proje sahibi katılımcıları davet eder; proje içeriğini yalnızca davet edilen kişiler görebilir. Projeye ait görevler, ilerleme ve belgeler bu kayıt üzerinden takip edilir.

(2) Platformda proje kapsamında veya projeden bağımsız kurum işleri için görevler oluşturulabilir. CÜNAM personeli kurum işleri için birbirine görev atayabilir. İlgili birimlere ait talep sayfalarından açılan kurum içi talepler ilgili birime yönlendirilir ve platformda takip edilir.

(3) Altyapı ve cihazlara ilişkin takip kayıtları platformda tutulur. LYS'deki cihaz randevularına ilişkin bildirimler platform üzerinden ilgili kişilere iletilir. Rezervasyon ve fiilî kullanım kayıtları LYS'de yürütülür.

MADDE 11 – Sunucu ve lisanslı yazılımlar

(1) Lisansların kullanıcı sayısı sınırlı olduğundan bazı programlarda mevcut sabit hesaplar yetkili iç kullanıcılar arasında ortak kullanılabilir. Bu hesap bilgileri, program sorumlusunun izin verdiği kişiler dışında paylaşılmaz. Ortak hesap kullanımı ilgili lisans sözleşmesinin izin verdiği ölçüde yapılır; ortak hesapla yapılan her kullanımda kullanıcının kimliği ve kullanım zamanı kayıt altına alınır.

(2) Program sorumlusu, projede görev alan veya ilgili programı kullanma yetkinliği bulunan CÜNAM iç kullanıcılarının erişimine karar verir ve gerekli hesap bilgisini izin verdiği kişilere iletir. Teknik işletim CÜNAM Bilgi İşlem birimince yürütülür.

MADDE 12 – Laboratuvar ve cihaz bilgisayarları

(1) Cihaza bağlı bilgisayarlar cihazın çalışması ve ilgili verilerin işlenmesi amacıyla kullanılır. Bu bilgisayarlar olağan kullanıcı bilgisayarı olarak başka amaçlarla kullandırılmaz.

(2) Cihaz bilgisayarlarında yazılım veya ağ ayarlarına ilişkin değişiklikler cihaz sorumlusu ile CÜNAM Bilgi İşlem biriminin bilgisi dışında yapılmaz.

MADDE 13 – Kiosk ve erişim terminalleri

(1) Kiosklar ve kart okuyucular LYS'de onaylanan cihaz kullanımının başlatılması, sonlandırılması ve ilgili onay işlemleri için kullanılır. Uygun cihazlarda onay sonrası üretilen tek kullanımlık erişim kodu da kullanılabilir. Kart ve kod yalnızca ilgili kişinin yetkili işlemi için kullanılır.

(2) Kiosk veya erişim terminalindeki arıza CÜNAM Bilgi İşlem birimine ve ilgili cihaz sorumlusuna bildirilir. Teknik arıza, cihaz sorumlusunun onayı olmadan cihaz çalıştırılmasına gerekçe oluşturmaz.

DÖRDÜNCÜ BÖLÜM

Veri Koruma, Süreklilik ve Olay Yönetimi

MADDE 14 – Verilerin korunması ve paylaşılması

(1) Kişisel veriler, proje verileri, sözleşmeyle korunan bilgiler ve yayımlanmamış araştırma çıktıları yalnızca yetkili kişilerce, amaçla sınırlı ve uygun güvenlik önlemleri alınarak işlenir. Üçüncü kişilere veri aktarımında veri sahibi birimin yetkisi, ilgili sözleşmeler ve uygulanabilir mevzuat dikkate alınır.

(2) Kurumsal verilerin kişisel e-posta adreslerine, onaylanmamış bulut hesaplarına veya taşınabilir ortamlara aktarımı yalnızca yetkilendirilmiş iş süreçleri kapsamında yapılır.

(3) Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberi ve CÜNAM FSMH Yönergesi uyarınca, CÜNAM bünyesinde yürütülen Ar-Ge projelerine ait ham veriler, çip/maske tasarımları, simülasyon kodları, patent taslakları ve müşteri analiz çıktıları CÜNAM Bilgi İşlem birimince onaylanmamış kişisel bulut depolama servislerine (Google Drive, Dropbox, WeTransfer vb.) yüklenemez ve kurum dışındaki yetkisiz kişisel e-posta adreslerine gönderilemez. İhlal hâlinde CÜNAM FSMH Yönergesi ve personelin tabi olduğu iş sözleşmesi ile ilgili mevzuat hükümleri uygulanır.

MADDE 15 – Kayıt ve denetim

(1) LYS ve kurumsal dijital süreç platformundaki işlem kayıtları ile sunucu ve uygulama erişim kayıtları, sistemlerin teknik imkânları ölçüsünde tutulur. Bu kayıtlara yalnızca görevli kişiler, yetkileri kapsamında erişebilir.

(2) Kayıtlar; güvenlik olaylarının incelenmesi, hizmet sürekliliğinin sağlanması ve yetkili denetimlerin yürütülmesi amacıyla kullanılır. Kişisel veriler gereğinden uzun süre tutulmaz; saklama ve silme işlemleri ilgili mevzuata göre yürütülür.

(3) 5651 sayılı Kanun ve ilgili mevzuat uyarınca, CÜNAM'ın kablolu veya kablosuz ağ altyapısından, sunucularından, LYS ve web sistemlerinden gerçekleştirilen erişimlere ait kaynak IP, hedef IP, port, oturum zamanı ve MAC adresi bilgilerini içeren trafik kayıtları, bütünlükleri değiştirilemeyecek şekilde zaman damgası ile imzalanarak iki yıl süreyle güvenli ortamda saklanır ve süre sonunda imha edilir.

MADDE 16 – Güncelleme ve değişiklik

(1) Desteklenen sistemlerde güvenlik güncellemeleri risk önceliğine göre uygulanır. Kritik güvenlik açığı veya aktif saldırı durumunda CÜNAM Bilgi İşlem birimi erişimi geçici olarak sınırlayabilir ve Müdürü derhâl bilgilendirir.

(2) Yeni bir servis, port veya üçüncü taraf entegrasyonu devreye alınmadan önce veri türü, ağ etkisi, yetkilendirme ve geri alma planı değerlendirilir.

(3) CÜNAM sunucu ve ağ altyapısı, yetkisiz erişimi ve zararlı trafiği engellemek amacıyla güvenlik duvarı (Firewall) ve ağ erişim kontrolü (NAC) sistemleri ile korunur. CÜNAM'ın dışa açık web, LYS ve sunucu altyapılarına yılda en az bir kez sızma testi (penetrasyon testi) yaptırılır; tespit edilen siber güvenlik açıkları CÜNAM Bilgi İşlem birimince giderilir.

MADDE 17 – Yedekleme ve geri yükleme

(1) LYS verileri ve CÜNAM sunucusu CÜNAM Bilgi İşlem birimince yedeklenir. Cihaz bilgisayarlarında oluşan ölçüm ve çalışma verileri bu merkezî yedekleme kapsamına dâhil değildir.

(2) LYS ve sunucu yedeklerinden geri yükleme gerektiğinde işlem CÜNAM Bilgi İşlem birimince yürütülür.

(3) Fidye yazılımı (Ransomware) ve fiziksel felaket risklerine karşı, LYS, kurumsal dijital süreç platformu ve kritik sunucu verilerinin periyodik yedeklerinden en az bir kopyası ağdan izole, fiziksel olarak güvenli bir ortamda çevrim dışı (Offline/Cold Backup) olarak saklanır. Yedeklerin geri yüklenebilirliği (Restore) 6 (altı) ayda bir test edilir.

MADDE 18 – Güvenlik olayı ve bildirim

(1) Şüpheli oturum, kimlik bilgisi sızıntısı, zararlı yazılım, kayıp cihaz, veri ifşası veya izinsiz değişiklik derhâl CÜNAM Bilgi İşlem birimine ve ilgili cihaz veya proje sorumlusuna bildirilir. Deliller korunur; gerekli görülmesi hâlinde etkilenen erişimler geçici olarak durdurulur.

(2) Müdür, olayın kapsamını ve gerekli hukuki bildirimleri yetkili birimlerle değerlendirir. Kullanıcı kendi başına dışarıya olay veya kişisel veri açıklaması yapamaz; ilgili kişilere ve kurumlara yapılacak bildirimler mevzuattaki yetki ve usullere göre gerçekleştirilir. Kişisel veri ihlallerinde ilgili kişiye ve Kişisel Verileri Koruma Kuruluna yapılacak bildirim, 6698 sayılı Kanunun 12 nci maddesinin beşinci fıkrası uyarınca en kısa sürede yapılır. Tespit edilen zafiyet ve siber olaylar, 7545 sayılı Siber Güvenlik Kanununun 7 nci maddesi uyarınca gecikmeksizin Siber Güvenlik Başkanlığına bildirilir. Bildirimleri Müdürün görevlendirdiği personel yürütür.

BEŞİNCİ BÖLÜM
Çeşitli ve Son Hükümler

MADDE 19 – Kullanıcıların bilgilendirilmesi

(1) Kullanıcılar, görevleriyle ilgili hesap ve şifre güvenliği, veri aktarımı ve güvenlik olayının bildirilmesi konusunda bilgilendirilir.

MADDE 20 – Uyumsuzluk ve itiraz

(1) Güvenlik açığı doğuran erişim, tehlike giderilene kadar gerekçesi kayıt altına alınarak geçici olarak durdurulabilir. Kalıcı yetki kaldırma veya diğer işlemler, ilgili kişinin açıklaması alınarak ilgili sözleşmeler ve uygulanabilir mevzuat çerçevesinde Müdür tarafından karara bağlanır.

(2) Kullanıcı, kendisine bildirilen erişim kararının gözden geçirilmesini CÜNAM Yönetim Kurulundan talep edebilir.

MADDE 21 – İstisnalar ve hüküm bulunmayan hâller

(1) İş gereği bir güvenlik kuralından sapılması gerektiğinde; gerekçe, risk, telafi edici tedbir, sorumlu ve bitiş tarihi kayıt altına alınır. Önemli istisnalar Yönetim Kurulunun onayına sunulur; acil durumlarda geçici tedbir Müdür tarafından uygulanır ve ilk toplantıda Yönetim Kuruluna bildirilir.

(2) Bu Yönergede hüküm bulunmayan hâllerde ilgili mevzuat, kuruluş protokolü ve Yönetim Kurulu kararları uygulanır.

MADDE 22 – Yürürlük

(1) Bu Yönerge, CÜNAM Yönetim Kurulu tarafından kabul edilip yayımlandığı tarihte yürürlüğe girer.

MADDE 23 – Yürütme

(1) Bu Yönerge hükümlerini CÜNAM Yönetim Kurulu adına CÜNAM Müdürü yürütür.