



Elektrik Üretim Sektöründe Siber Güvenlik Yetkinlik Modeli

Taslak Teknik Kontrol Maddeleri

EPDK, taslak kontrol maddelerinde ekleme, düzenleme ve çıkarma yetkisine sahip tek kuruluştur.

Elektrik Üretimi 100MW üstü lisans sahibi işletmeler için minimum uygulanacak kontroller Seviye 1 olarak belirlenmiştir.

Seviye	Açıklama	Hedeflenen Tamamlama Süresi (Öz Denetim/Fark Analizlerinin Tamamlanmasından Sonra)
Seviye 1	Giriş seviyesi kontroller bu grupta yer almaktadır. İlgili kontrollerin hali hazırda uygulandığı ya da kolayca uygulanabileceği değerlendirilen maddeler bu grupta toplanmıştır. Bu grupta yer alan maddeleri uygulamak zorunludur.	18 Ay
Seviye 2	İkinci aşama kontroller bu grupta yer almaktadır. İlgili kontrollerin uygulanabilmesi için kurum içi değişikliklerin yapılması gerekli kontroller bu grupta toplanmıştır. Bu grupta yer alan maddeleri uygulamak zorunludur.	24 Ay
Seviye 3	Üçüncü seviye kontroller bu grupta yer almaktadır. Bu grupta yer alan kontroller yeni bir projelendirme ya da uzun soluklu değişim gerektirmektedir. Bu grupta yer alan maddeleri uygulamak zorunludur.	30 Ay
Ek Kontroller	Zorluk derecesi yüksek ya da uygulanmasının faydalı olabileceği değerlendirilen kontroller bu grupta toplanmış olup zorunlu değildir.	

Tanım	Açıklama
Hardwired	Fiziksel kanallar üzerinden sağlanan haberleşme türü
SIS	Safety Instrument System, emniyet kontrol sistemi Elektrik üretim tesislerinde tümünden safety/emniyet kontrol sistemleri olabileceği gibi, doğrudan safety/emniyet PLC'leri olarak da ele alınır.
SIL	Safety Integrity Level
Elektrik Üretim endüstriyel kontrol sistemleri (EKS)	Elektrik Üretim santrali içerisinde olan tüm endüstriyel kontrol sistemlerini içerir. Tüm ana prosesler, destekleyici prosesler ve yan proseslere hizmet eden DCS, SCADA teknolojileri ve bu bileşenlere hizmet eden ayrı kontrol sistemleri kapsama dahildir.
Kontrol Odası, Board Odası, Kumanda Odası	DCS ve SCADA izleme ve/veya kumanda odasını ifade eder.
DCS Odaları	Endüstriyel operasyonların gerçekleştirildiği kontrol odalarını ve bu işleme hizmet eden ana ve destekleyici tüm sistemleri barındıran fiziksel alanları ifade eder.
Kontrol ekipman odaları	DCS, PLC, RTU, Kontrolcü, IED içeren Panelleri veya bunları izleyen istemci/sunucuların olduğu odaları ifade eder.
OPC	Ole for Process Control Server-Client tabanlı Endüstriyel haberleşme standardı
Endüstriyel Ağlarda Merkezi Yönetim	Farklı endüstriyel kontrol sistemlerinin merkezi olarak izlendiği yapıyı ifade eder. Merkezi operasyon noktasında bulunan ağlar ve bileşenler yetkinlik modeli kapsamındadır.
OT Sanallaştırma	OT ve OT-DMZ bileşenlerinde kullanılan sanallaştırma altyapısını ifade eder.
SCADA Yazılımı	PLC, RTU, Kontrolcü, IED lardan bağımsız Operator ve/veya Serverlara kurulan, PLC, RTU, Kontrolcü, IED ile gerçek zamanlı veri haberleşmesi yapan ve değerleri Operatörün takip edebileceği gibi görselleştiren endüstriyel yazılımlardır.
DCS	Dağıtık kontrol sistemi
Balance of Plant	Santral bünyesinde kullanılan destekleyici operasyonları ve operasyonlara ait bileşenleri ifade eder.
Utilities	Santral bünyesinde kullanılan destekleyici operasyonları ve operasyonlara ait bileşenleri ifade eder.

ICCP	Inter-Control Center Communication Protocol
Sunucu Odası veya Veri Merkezi (Fiziksel Güvenlik Başlığı)	Endüstriyel sistemleri barındıran sistem odası ve veri merkezi ifade edilmektedir.
Bypass	Mevcut herhangi bir güvenlik mekanizmasının atlatılmasını ifade eder.

Endüstriyel Ağ Güvenliği				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EAG-1	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 1	Elektrik üretim ana endüstriyel kontrol sistemlerinde (EKS) hizmet veren bileşenlerin bulunduğu tüm alanlara (ana kontrol odası, kontrol odası, kumanda odası, DCS odası, board odası vb.) yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalı (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) veya fiziksel güvenlik önlemleri ile yetkisiz erişimler engellenmelidir. Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-2	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 1	Elektrik üretim destekleyici endüstriyel kontrol sistemlerinde (EKS) (Balance of Plant, utilities, harici kontrol sistemleri) hizmet veren bileşenlerin bulunduğu tüm alanlara (ana kontrol odası, kontrol odası, kumanda odası, DCS odası, board odası vb.) yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalı (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) veya fiziksel güvenlik önlemleri ile yetkisiz erişimler engellenmelidir. Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-3	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Erişim Kontrolleri	Seviye 1	Elektrik üretim tesisi bünyesinde izleme ve raporlama amaçlı kullanılan (GKC, RITM, verimlilik vb.) bileşenlerin bulunduğu tüm alanlara (ana kontrol odası, kontrol odası, kumanda odası, DCS odası, board odası vb.) yetkisiz kişi ve cihazların endüstriyel ağa girişi (Network Access) kısıtlanmalı (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) veya fiziksel güvenlik önlemleri ile yetkisiz erişimler engellenmelidir. Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-4	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim ana endüstriyel kontrol sistemleri (EKS), güvenlik duvarı ile korunmalıdır. (Referans_Topoloji_EÜ_RES: EKS-GD-01, Referans_Topoloji_EÜ_HES: EKS-GD-01, Referans_Topoloji_EÜ_Termik: EKS-GD-01, Referans_Topoloji_EÜ_GES: EKS-GD-01) Bu güvenlik duvarı sadece endüstriyel ağların izolasyonu/ayrıştırılması için konumlandırılmalı ve KBS güvenlik duvarından farklı olmalıdır. Kullanılan güvenlik duvarı ilgili kuruluşun endüstriyel kontrol sistemleriyle entegrasyonda kullanılan protokollerini desteklemelidir.
EAG-5	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), kontrol seviyesi bileşenleri (PLC, CPU, kontrolcü) endüstriyel kontrol sistemlerine özel güvenlik bileşenleriyle korunmalıdır.
EAG-6	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 3	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), iki farklı kontrol sisteminin entegrasyonunda kullanılan veriler kontrol amaçlı kullanılıyorsa bu veri transferi hardwired kanallar üzerinden sağlanmalıdır.
EAG-7	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 3	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), iki farklı kontrol sisteminin entegrasyonu ethernet tabanlı sağlanıyorsa ilgili entegrasyon sadece izleme amaçlı kullanılmalı veya bu entegrasyonlar bir güvenlik katmanından geçirilmelidir.

EAG-8	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) kontrol odaları ile kontrol ekipmanlarının olduğu odalar arasında Layer2 bağlantı olması durumunda, her iki noktada aynı ağ güvenlik kontrolleri uygulanıyor olmalıdır.
EAG-9	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar ve harici ağlar arasındaki (güvensiz ağlar) haberleşmeler güvenlik duvarı (Referans_Topoloji_EÜ_RES: EKS-GD-01, Referans_Topoloji_EÜ_HES: EKS-GD-01, Referans_Topoloji_EÜ_Termik: EKS-GD-01, Referans_Topoloji_EÜ_GES: EKS-GD-01) üzerinden sağlanmalıdır. Bu güvenlik duvarı endüstriyel ağı izole eden güvenlik duvarıdır.
EAG-10	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), elektrik üretim santralinin farklı kontrol sistemleri ile ICCP üzerinden veri okuma entegrasyonları endüstriyel ağı izole eden güvenlik duvarı (Referans_Topoloji_EÜ_RES: EKS-GD-01, Referans_Topoloji_EÜ_HES: EKS-GD-01, Referans_Topoloji_EÜ_Termik: EKS-GD-01, Referans_Topoloji_EÜ_GES: EKS-GD-01) üzerinden sağlanmalıdır.
EAG-11	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), elektrik üretim santralinin farklı kontrol sistemleri ile ICCP üzerinden veri yazma entegrasyonları, ICCP protokolünü tanıyan ve sadece belirli parametrelere izin verebilen bir güvenlik duvarı (Referans_Topoloji_EÜ_RES: EKS-GD-01, Referans_Topoloji_EÜ_HES: EKS-GD-01, Referans_Topoloji_EÜ_Termik: EKS-GD-01, Referans_Topoloji_EÜ_GES: EKS-GD-01) veya benzeri güvenliği sağlayabilen bir güvenlik bileşeni üzerinden sağlanmalıdır.
EAG-12	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim tesisi bünyesinde elektrik iletim şebekesine bağlantı noktası olan şalt sahası endüstriyel kontrol sistemlerinde (EKS) hizmet veren bileşenlerin bulunduğu tüm alanlara yetkisiz kişi ve cihazların endüstriyel ağı girişi (Network Access) kısıtlanmalı (Port security, kullanılmayan portların devre dışı bırakılması, fiziksel olarak kapatılması vb.) veya fiziksel güvenlik önlemleri ile yetkisiz erişimler engellenmelidir. Bu kontroller hem kablolu hem de kablosuz ağlar için uygulanmalıdır.
EAG-13	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim tesisi bünyesinde elektrik iletim şebekesine bağlantı noktası olan şalt sahası endüstriyel kontrol sistemlerinde (EKS), iletim şebekesi ile ağ tabanlı bağlantılar bir güvenlik katmanı üzerinden geçirilmelidir.
EAG-14	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim tesisi bünyesinde doğal gaz dağıtım ya da iletim şebekesine bağlantılar bulunuyorsa, ilgili bağlantılar yükümlü kuruluşa ait bir güvenlik katmanı üzerinden geçirilmeli ya da bağlantılar hardwired kanallar üzerinden sağlanmalıdır.

EAG-15	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Ek kontrol	Elektrik üretim tesisi bünyesinde elektrik iletim şebekesine bağlantı noktası olan şalt sahası endüstriyel kontrol sistemlerinde (EKS) güvenlik duvarı kullanılması durumunda bu güvenlik duvarının (Referans_Topoloji_EÜ_RES: EKS-GD-01, Referans_Topoloji_EÜ_HES: EKS-GD-01, Referans_Topoloji_EÜ_Termik: EKS-GD-01, Referans_Topoloji_EÜ_GES: EKS-GD-01) yetkisiz endüstriyel komutları durdurabilecek yeterlilikle olmalıdır. (IEC 104, DNP3 protokolleri ile elektrik açma/kesme operasyonları vb.)
EAG-16	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) her bir endüstriyel ağa ilişkin mantıksal topolojiler her bir endüstriyel üreticinin mimarisi göz önünde bulundurularak katmanlı güvenlik yaklaşımına göre tasarlanmalı ve uygun şekilde dokümente edilmelidir.
EAG-17	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) her bir endüstriyel ağa ilişkin fiziksel topolojiler dokümente edilmelidir.
EAG-18	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel bileşenlere güvensiz ağlar ya da yarı güvenli ağlar (DMZ: Demilitarized zone) üzerinden olan erişim trafiği bir saldırı tespit katmanından geçirilmelidir. Bunu sağlamak adına mevcut güvenlik bileşenlerinde IDS imzaları devreye alınabileceği gibi alternatif olarak açık kaynak kodlu teknolojiler de kullanılabilir.
EAG-19	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 3	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlarda trafik aynalanması (mirroring) yöntemi ile saldırı tespiti gerçekleştirilebilmelidir.
EAG-20	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Kesme	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağları izole etmek/ayırıştırmak için konumlandırılan güvenlik duvarı üzerinde (Referans_Topoloji_EÜ_RES: EKS-GD-01, Referans_Topoloji_EÜ_HES: EKS-GD-01, Referans_Topoloji_EÜ_Termik: EKS-GD-01, Referans_Topoloji_EÜ_GES: EKS-GD-01) endüstriyel protokollere yönelik tehditleri de içeren IPS ve antivirüs vb. güvenlik önlemleri devreye alınmalıdır.
EAG-21	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde bulunan bileşenler görevlerine veya endüstriyel üreticinin sağladığı katmanlı yapıya göre sanal ağlara (VLAN) ayrılmalı ve bu ağlar arasında geçiş kontrolleri uygulanmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-22	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) mühendislik operasyonları kapsamında taşınabilir mühendislik iş istasyonları kullanılıyorsa, bu bileşenler endüstriyel ağlardan izole edilmelidir. İzole edilemediği durumlarda ise kullanılmadığı sürece kapalı tutulmalıdır.

EAG-23	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) mühendislik operasyonları kapsamında kontrol sistemlerinin bir parçası olarak kullanılan mühendislik iş istasyonları kullanılmadığı sürece kapalı tutulmalıdır. Mühendislik yetkisinin sadece mühendislik operasyonlarında kullanıldığı garanti altına alınmalıdır. Mümkün ise de Mühendislik istasyonları yetkisiz personelin girmeyeceği ayrı bir odada çalıştırılmalıdır.
EAG-24	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) enstrümanların konfigüre edildiği bileşenler izole ağlar üzerinde ana kontrol sisteminin haricinde konumlandırılmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-25	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) enstrümanların konfigüre edildiği bileşenler katmanlı güvenlik mimarisine uygun olarak ilgili bileşenlere en yakın katmanda konumlandırılmalıdır.
EAG-26	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlardan kurumsal ağlara doğru olan haberleşmeler bu haberleşmelere özel oluşturulmuş OT-DMZ ağları ya da izole sanal ağlar (VLAN) üzerinden sağlanmalıdır. Aynı şekilde kurumsal ağlardan endüstriyel ağlara doğru olan haberleşmeler de OT-DMZ ağları ya da izole sanal ağlar (VLAN) üzerinden sağlanmalıdır.
EAG-27	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) sanal ağların (VLAN) devreye alınmasını takiben ağ ve güvenlik cihazlarının yönetim arayüzleri de (management interface) ayrı bir sanal ağ üzerinde konumlandırılmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-28	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dağıtık uç istasyon yapısında olan santrallerin (RES ve GES) her bir uç noktasında bulunan endüstriyel ağlar farklı bir alt ağ olarak oluşturulmalıdır.
EAG-29	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) altyapısında kontrol odaları ve kontrol ekipman odaları bünyesinde endüstriyel protokol trafiği ve diğer ağ trafikleri (kamera, fiziksel güvenlik vb.) fiziksel olarak ayrı ağ cihazları üzerinden taşınmalıdır.
EAG-30	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Ek kontrol	Endüstriyel ağlarla iletişim halinde olan tüm KBS bileşenleri ayrı bir sanal ağ (VLAN) içerisinde konumlandırılmalı ve OT-DMZ ağı üzerinden endüstriyel ağlar ile haberleşmelidir. (PI, OPC, verimlilik, Güvenli Uzak Erişim vb.)
EAG-31	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Endüstriyel ağlar ve KBS ağları arasında haberleşmenin yönü endüstriyel ağdan kurumsal ağa olacak şekilde OT-DMZ üzerinden sağlanmalıdır. Kurumsal ağlardan endüstriyel ağlara doğru veri çekme operasyonlarının gerekli olması durumunda bu veri akışı telafi edici kontrollerle birlikte gerçekleştirilmelidir.

EAG-32	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 1	Her bir endüstriyel ağ içerisinde yer alan sunucu ve uygulamalar doğrudan internet üzerinden erişilebilir durumda olmamalıdır.
EAG-33	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 1	Endüstriyel ağlarla iletişimi olan tüm bileşenlerin doğrudan internete olan erişimleri sonlandırılmalıdır.
EAG-34	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Seviye 1	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine internet üzerinden gerçekleştirilecek tüm uzak erişimler öncelikli olarak KBS/kurumsal ağ üzerinde sonlandırılmalıdır. (VPN vb.) Bu uzak erişim yöntemleri üreticiler, çalışanlar ve alt yükleniciler için farklı yetkilendirme politikalarını destekleyebilmelidir. KBS ağı üzerinden endüstriyel ağlara yönelik uzak erişimler OT-DMZ ağı içerisinde konumlandırılmış güvenli bir atlama noktası/sunucusu/uygulaması üzerinden kontrollü olarak sağlanmalıdır. Uzaktan erişimlere ilişkin tüm süreçler diğer mevcut teknik maddelere uyumlu olarak işletilmelidir. (Olay yönetimi ve süreklilik, kimlik ve erişim yönetimi vb.)
EAG-35	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yapılacak uzak erişimler için bu işe özelleşmiş teknolojiler kullanılmalıdır. (Oturma kaydetme, oturma yönetimi, çift faktörlü doğrulama, güvenli dosya transferi vb.)
EAG-36	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS), endüstriyel üreticilerin doğrudan kendi sistemleri üzerinden bağlantı yapması engellenmelidir. Yapılacak olan uzak erişimler yükümlü kuruluş güvenlik katmanlarından geçirilmelidir.
EAG-37	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Seviye 2	Elektrik üretim tesisi kapsamında endüstriyel operasyonların yönetiminde sözleşmelerle tariflenen üretici tabanlı uzaktan yönetim ve izleme işlemleri yapılıyorsa, bu uzak bağlantılar yükümlü kuruluş güvenlik katmanlarından geçirilmelidir.
EAG-38	Endüstriyel Ağ Güvenliği	Endüstriyel Ağa Uzak Erişim	Seviye 2	Elektrik üretim tesisi kapsamında endüstriyel operasyonların yönetiminde sözleşmelerle tariflenen üretici tabanlı uzaktan yönetim ve izleme işlemleri yapılıyorsa, bu uzak erişimler için çok faktörlü kimlik doğrulama adımları kullanılmalıdır.
EAG-39	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tüm güvensiz servisler (açık metin protokoller, uzak erişim servisleri, güncelliğini yitirmiş protokoller) periyodik denetim ya da ağ trafiğinin analizi ile tespit edilmelidir.
EAG-40	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Güvenli Konfigürasyon	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tespit edilen BT tabanlı (TELNET, HTTP, TFTP, vb.) güvensiz servisler devre dışı bırakılmalıdır.
EAG-41	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Güvenli Konfigürasyon	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde tespit edilen gereksiz veya kullanılmayan servisler devre dışı bırakılmalıdır.
EAG-42	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağlar üzerinde mevcut varlıkların servisleri sürekli olarak izlenmelidir.

EAG-43	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) güvenli ve güvensiz ağlar arasında mevcut olan koruma mekanizmalarının bypass edilmesine olanak tanıyabilecek tüm dual-homed arayüzler (interface) devre dışı bırakılmalıdır. İkinci bir arayüz kullanılmasını zorunlu kılan bir durum mevcut ise söz konusu arayüzün bağlantısı güvenlik duvarı (Referans_Topoloji_EÜ_RES: EKS-GD-01, Referans_Topoloji_EÜ_HES: EKS-GD-01, Referans_Topoloji_EÜ_Termik: EKS-GD-01, Referans_Topoloji_EÜ_GES: EKS-GD-01) üzerinden kontrollü olarak sağlanmalıdır.
EAG-44	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel üreticinin tasarım gereklilikleri haricinde Seviye-2 ile Seviye-1 (Purdue modeline göre) ağlar arasında mevcut olan koruma mekanizmalarını bypass edilmesine olanak tanıyabilecek tüm dual-homed arayüzler interface'ler devre dışı bırakılmalıdır. İkinci bir arayüz kullanılmasını zorunlu kılan bir durum mevcut ise söz konusu arayüzün bağlantısı güvenlik duvarı üzerinden kontrollü olarak sağlanmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EAG-45	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Saldırı Tespiti/İzleme	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağ içerisinde bulunan ağ cihazları "Olay Yönetimi ve Süreklilik" başlığının ilgili maddelerini karşılamalıdır. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
EAG-46	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağların dışına çıkan endüstriyel veriler şifreli kanallar üzerinden taşınmalıdır. (Örn: OPC-UA Şifreleme, SSL vb.)
EAG-47	Endüstriyel Ağ Güvenliği	Endüstriyel Ağ İzolasyonu ve Segmentasyonu	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel ağların izolasyon ve segmentasyonunda yazılım tabanlı teknolojilere ek olarak donanım tabanlı teknolojiler de devreye alınmalıdır.
EAG-48	Endüstriyel Ağ Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan tüm ağ cihazları Tehdit ve Zafiyet Yönetimi başlığına uygun olarak işletilmelidir. Yükümlü kuruluşlar acil olan yamalar dışında yılda en az bir kez yama ve güncelleme yapmalıdırlar. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
EAG-49	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, endüstriyel ağlardan kurum dışına çıkarılacak veriler tek yönlü, şifreli kanallar üzerinden ve katmanlı güvenlik ilkelerine uygun şekilde çıkarılmalıdır. Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.

EAG-50	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, dijital ikiz sistemlerine aktarılan verilerin güvenliği sözleşmelerle garanti altına alınmalıdır. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-51	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, dijital ikiz sistemleri üzerinden veri ifşası olmayacak kontroller devreye alınmalıdır. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-52	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, bu sistemin üreticilerinin "Tedarikçi Yönetimi" başlığı altında mevcut kontrollere uygun çalıştığı garanti altına alınmalıdır. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-53	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, dijital ikiz sistemlerinden endüstriyel ağlara doğru bir erişim tanımlanmadığı garanti altına alınmalıdır. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-54	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, dijital ikiz sistemlerinin bulunduğu bulut ortamları için CB-DDO Bulut Güvenliği kontrolleri uygulanmalıdır. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>

EAG-55	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa; - Erişen personel, yetki ve yetkinlik düzeyleri - Erişim, işlem ve ağ trafiği iz kayıtlarının izlenmesi - Güncelleme durum alarmları - Siber olay alarmları - Performans ve kapasite göstergeleri kurum tarafından kontrol edilmelidir. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-56	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, aynı bulut ortamını kullanan kurumların sistemleri ağ seviyesinde birbirlerinden mantıksal ve/veya fiziksel olarak izole edilmelidir. Kurumların yalnızca kendilerine ait veriye erişim imkânı sağlanmalıdır. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-57	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, bulut hizmeti kapsamında, ihtiyaç olması durumunda şablon olarak kullanılan imajların geri döndürülemeyecek şekilde silinmesine servis sağlayıcı tarafından imkân tanınmalıdır. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-58	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan bellek bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>

EAG-59	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, bulut sistemi yönetim konsoluna sadece izin verilen ağlardan erişim garanti altına alınmalıdır. (SSL-VPN, IPSEC VPN vb.) <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-60	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan disk bölgeleri otomatik olarak servis sağlayıcı tarafından geri döndürülemeyecek şekilde silinmelidir. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-61	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, paylaşımlı/bulut ortamdan hizmet sağlayan servis sağlayıcılar hizmetin sonlanması durumunda hizmet alan tarafa ait profil ayarları, hizmet raporları vb. hizmete ilişkin tanımları silmelidir. Bulut sistemlerde barındırılan veriler, kullanımının sonlandırılması durumunda sistemlerden geri getirilemeyecek şekilde silinmelidir. <i>Bu madde kapsamında kullanılan dijital ikiz ve bulut çözümleri 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Madde 3 kapsamında ele alınmalıdır.</i>
EAG-62	Endüstriyel Ağ Güvenliği	Dijital İkiz Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) dijital ikiz sistemleri kullanılıyorsa, bulut sistemlerde gerçekleştirilen yönetsel işlemler kayıt altına alınmalı ve değişmezliği sağlanmalıdır.
EAG-63	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, endüstriyel kablosuz ağ protokolleri (Wireless HART, ISA100 vb.) araya girme saldırılarına karşı dirençli olmalıdır.
EAG-64	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, endüstriyel kablosuz ağ protokolleri (Wireless HART, ISA100 vb.) servis sonlandırma saldırılarına karşı dirençli olmalıdır.
EAG-65	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, endüstriyel kablosuz ağ protokolleri (Wireless HART, ISA100 vb.) kimlik doğrulama yöntemlerini desteklemelidir.
EAG-66	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, kablosuz ağ trafiği şifreli kanallar üzerinden sağlanmalıdır.

EAG-67	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, endüstriyel kablosuz ağ protokolleri (Wireless HART, ISA100 vb.) parola tahmin saldırılarına karşı dirençli olmalıdır.
EAG-68	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, bu ağlar geleneksel kablosuz ağlardan (WiFi vb.) mantıksal ve fiziksel olarak izole edilmelidir.
EAG-69	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, kablosuz ağ üzerinden taşınan endüstriyel veriler kontrol mimarisinde sadece izleme amaçlı kullanılmalıdır.
EAG-70	Endüstriyel Ağ Güvenliği	Endüstriyel Kablosuz Ağ Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), endüstriyel kablosuz ağlar kullanılıyorsa, kablosuz ağ mimarisinde kullanılan tüm ağ bileşenleri "Endüstriyel Ağ Güvenliği" kontrollerine uyumlu olmalıdır.
EAG-71	Endüstriyel Ağ Güvenliği	Harici Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim bünyesinde kullanılan harici izleme sistemleri (GKC, RITM vb.) ve destek sistemleri (balance of plant, utilities) elektrik üretim endüstriyel kontrol sistemlerinden (EKS) mantıksal olarak izole edilmelidir.
EAG-72	Endüstriyel Ağ Güvenliği	Harici Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim bünyesinde kullanılan harici izleme sistemleri (GKC, RITM vb.) ve destek sistemleri (balance of plant, utilities) elektrik üretim endüstriyel kontrol sistemleriyle entegre olması gerekiyorsa bu entegrasyon bir ağ güvenlik katmanı üzerinden geçirilmelidir.
EAG-73	Endüstriyel Ağ Güvenliği	Harici Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim bünyesinde kullanılan harici izleme sistemleri (GKC, RITM vb.) ve destek sistemleri (balance of plant, utilities) doğrudan internete erişmemeli ve internet üzerinden erişilebilir olmamalıdır.
EAG-74	Endüstriyel Ağ Güvenliği	Harici Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim bünyesinde kullanılan harici sistemler (kamu veya özel sektör entegrasyonları, yerli kömür teşvikleri vb.) doğrudan internete erişmemeli ve internet üzerinden erişilebilir olmamalıdır.
EAG-75	Endüstriyel Ağ Güvenliği	Harici Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim bünyesinde kullanılan harici sistemler (kamu veya özel sektör entegrasyonları, yerli kömür teşvikleri vb.) elektrik üretim endüstriyel kontrol sistemleriyle entegre olması gerekiyorsa bu entegrasyon bir ağ güvenlik katmanı üzerinden geçirilmelidir.
EAG-76	Endüstriyel Ağ Güvenliği	Büyük Veri Analitiği Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) büyük veri analitiği sistemleri veya kestirimci bakım sistemleri kullanılıyorsa, endüstriyel ağlardan KBS ağına gönderilecek veriler tek yönlü, şifreli kanallar üzerinden ve katmanlı güvenlik ilkelerine uygun şekilde çıkarılmalıdır.

EAG-77	Endüstriyel Ağ Güvenliği	Büyük Veri Analitiği Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) büyük veri analitiği sistemleri veya kestirimci bakım sistemleri kullanılıyorsa, KBS ağındaki sistemler en az gerçek sistem kadar mantıksal olarak izole edilmelidir.
EAG-78	Endüstriyel Ağ Güvenliği	Büyük Veri Analitiği Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) büyük veri analitiği sistemleri veya kestirimci bakım sistemleri kullanılıyorsa, veri analitiği sistemleri üzerinden veri ifşası olmayacak kontroller devreye alınmalıdır.
EAG-79	Endüstriyel Ağ Güvenliği	Büyük Veri Analitiği Sistemlerinin Entegrasyonu	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) büyük veri analitiği sistemleri veya kestirimci bakım sistemleri kullanılıyorsa, bu sistemlere ilişkin tedarikçi kullanılması durumunda bu sistemin üreticilerinin "Tedarikçi Yönetimi" başlığı altında mevcut kontrollere uygun çalıştığı garanti altına alınmalıdır. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
EAG-80	Endüstriyel Ağ Güvenliği	Büyük Veri Analitiği Sistemlerinin Entegrasyonu	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) büyük veri analitiği sistemleri veya kestirimci bakım sistemleri kullanılıyorsa, endüstriyel ağlara doğru bir erişim tanımlanmadığı garanti altına alınmalıdır.
EAG-81	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Merkezi Yönetim	Seviye 1	Elektrik üretim operasyonları kapsamında aynı kuruluş bünyesinde farklı lisansa sahip santralleri merkezi olarak izleniyor veya yönetiliyorsa, merkezi izleme noktasında bulunan ağlar "Endüstriyel Ağ Güvenliği" başlığı altındaki teknik kontrollere uyumlu olmalıdır.
EAG-82	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Merkezi Yönetim	Seviye 2	Elektrik üretim operasyonları kapsamında aynı kuruluş bünyesinde farklı lisansa sahip santralleri merkezi olarak izleniyor veya yönetiliyorsa, izleme kapsamında olan her bir endüstriyel kontrol sistemi ağ birbirinden izole edilmelidir. Bu ağlar arasında fiziksel ve mantıksal ayrıştırmalar yapılmalıdır.
EAG-83	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Merkezi Yönetim	Seviye 2	Elektrik üretim operasyonları kapsamında aynı kuruluş bünyesinde farklı lisansa sahip santralleri merkezi olarak izleniyor veya yönetiliyorsa, izleme kapsamında olan her bir endüstriyel kontrol sisteminin merkeze olan bağlantıları şifreli kanallar üzerinden sağlanmalıdır.
EAG-84	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Merkezi Yönetim	Seviye 1	Elektrik üretim operasyonları kapsamında aynı kuruluş bünyesinde farklı lisansa sahip santralleri merkezi olarak izleniyor veya yönetiliyorsa, izleme kapsamında olan her bir endüstriyel kontrol sistemine uzak bağlantılar gerçekleştiriliyorsa, bu erişimler "Endüstriyel Ağ Güvenliği" başlığı altındaki teknik kontrollere uyumlu gerçekleştirilmelidir. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
EAG-85	Endüstriyel Ağ Güvenliği	Endüstriyel Ağlarda Merkezi Yönetim	Seviye 2	Elektrik üretim operasyonları kapsamında aynı kuruluş bünyesinde farklı lisansa sahip santralleri merkezi olarak izleniyor veya yönetiliyorsa, merkezi operasyon noktasında ağa giriş kontrolleri uygulanmalıdır.

Endüstriyel İstemci ve Sunucu Güvenliği

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İSG-1	Endüstriyel İstemci ve Sunucu Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucular için endüstriyel üretici tarafından onaylanan ve operasyonel sürekliliği tehlikeye atmayacak uç nokta (endpoint) güvenlik önlemleri (kötü amaçlı yazılım koruma uygulamaları, uç nokta tehdit tespit sistemi, uç nokta güvenlik duvarı vb.) tanımlanmalı ve uygulanmalıdır.
İSG-2	Endüstriyel İstemci ve Sunucu Güvenliği	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren istemciler için endüstriyel üretici tarafından onaylanan ve operasyonel sürekliliği tehlikeye atmayacak uç nokta (endpoint) güvenlik önlemleri (kötü amaçlı yazılım koruma uygulamaları, uç nokta tehdit tespit sistemi, uç nokta güvenlik duvarı vb.) tanımlanmalı ve uygulanmalıdır.
İSG-3	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren istemcilerde harici medya kullanımları devre dışı bırakılmalıdır.
İSG-4	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucularda harici medya kullanımları devre dışı bırakılmış olmalıdır.
İSG-5	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Medya Güvenliği	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde yeni nesil USB tabanlı saldırılara karşı önlem alınmalıdır. (Rubber Ducky vb.)
İSG-6	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Olay Tespiti ve Yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde "Olay Yönetimi ve Süreklilik" başlığı altındaki maddelere uygun olarak loglar tutulmalı ve yönetilmelidir. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
İSG-7	Endüstriyel İstemci ve Sunucu Güvenliği	Mobil Cihaz Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren taşınabilir mühendislik iş istasyonları (dizüstü vb.) ilgili kuruluş envanterine kayıtlı olmalıdır. Mühendislik operasyonlarında alt yüklenicilere ait güvensiz iş istasyonları endüstriyel ağa dahil edilmemeli ve EKS bileşenlerine bağlanmamalıdır. Kuruluşa ait taşınabilir mühendislik iş istasyonlarının güvenlik seviyesi kuruluş içi ve kuruluş dışında aynı olmalıdır.
İSG-8	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucu Operasyon Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren mühendislik iş istasyonları günlük operasyonel işlerde kullanılmamalıdır. (E-posta vb.)
İSG-9	Endüstriyel İstemci ve Sunucu Güvenliği	Veri Koruma	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde disk şifreleme yöntemleri uygulanmalıdır.
İSG-10	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde güvenli BIOS yapılandırmaları devreye alınmalıdır.
İSG-11	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde sadece yetkili kullanıcıların uygulama kurmasına izin verilmelidir.

İSG-12	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde sadece güvenlik onayından geçmiş uygulamaların yüklenmesine ve kullanılmasına izin verilmelidir.
İSG-13	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler için kuruluşa özel güvenli bir kurulum imaj dosyası oluşturulmalı, periyodik olarak kontrol edilmeli ve güncellenmelidir.
İSG-14	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde internet üzerinden güvensiz uzak erişime imkan verecek yazılım ve servisler bulundurulmamalıdır.
İSG-15	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunuculara bulundukları ağ içerisinde uzak erişim (VNC, SSH, RDP vb.) yapılması durumunda ek güvenlik kontrolleri uygulanmalıdır. (sanal ağ ayırıştırma, güvenli atlama noktası, uç nokta güvenlik duvarı ile erişim kısıtlamaları vb.)
İSG-16	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucu Operasyon Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan tüm uygulamalar lisanslı olmalıdır.
İSG-17	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Olay Tespiti ve Yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler merkezi bir zamanlama sunucusundan senkronize edilmelidir. Bu senkronizasyon işlemi sırasında ağ seviyesinde sadece gerekli servis ve portlara izin verilmelidir.
İSG-18	Endüstriyel İstemci ve Sunucu Güvenliği	GPS Güvenliği	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler için kullanılan merkezi zamanlama sunucusunun GPS tabanlı olması halinde, GPS temelli saldırılara karşı koruma önlemleri alınmalıdır.
İSG-19	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan kötü amaçlı yazılım koruma uygulamaları endüstriyel üreticinin de onayladığı aralıklarla güncellenmelidir. Bu aralıklar 4 aydan daha uzun süreli olarak tanımlanmamalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
İSG-20	Endüstriyel İstemci ve Sunucu Güvenliği	Zararlı Yazılımlardan Korunma	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan kötü amaçlı yazılım koruma uygulamaları yüksek yetkili kullanıcılar tarafından da dahil olmak üzere devre dışı bırakılamamalıdır.
İSG-21	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güncelleme/Yama Yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerin işletim sistemleri endüstriyel üreticinin de onayladığı tanımlı aralıklarla güncellenmelidir. Yükümlü kuruluşlar yılda en az bir kez güncelleme yapmalıdırlar. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)

İSG-22	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güncelleme/Yama Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemciler üzerinde bulunan uygulamalar, üretici güncelleme ve yamalarının yayınlanmış olma ihtimaline karşı belirlenen aralıklarla kontrol edilmelidir. Güvenlik açısından önem arz eden güncellemeler endüstriyel üretici gözetiminde gerçekleştirilmelidir. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
İSG-23	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerin tüm gereksiz kablolu ve kablosuz ağ arayüzleri devre dışı bırakılmalıdır. Ek olarak tüm gereksiz servis ve portlar devre dışı bırakılmalıdır.
İSG-24	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerin ağ servisleri yönetiminde "Endüstriyel Ağ Güvenliği" başlığının ilgili maddelerine uygun hareket edilmelidir. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
İSG-25	Endüstriyel İstemci ve Sunucu Güvenliği	İstemci ve Sunucularda Güvenli Konfigürasyon	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde IPv6 ağ arayüzleri devre dışı bırakılmalıdır.
İSG-26	Endüstriyel İstemci ve Sunucu Güvenliği	Veri Koruma	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde imha yönetimi kuruluşun belirlediği politikalar doğrultusunda gerçekleştirilmelidir.
İSG-27	Endüstriyel İstemci ve Sunucu Güvenliği	Beyaz Liste Uygulamaları	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) içerisinde hizmet veren sunucu ve istemcilerde beyaz liste (Whitelisting) uygulamaları devreye alınmalıdır.
İSG-28	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda endüstriyel etki alanı ile KBS etki alanı birbirinden tamamiyle izole edilmelidir. (Bu amaçla trust, parent-child, farklı OU gibi yöntemler kullanılmamalıdır.)
İSG-29	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, endüstriyel etki alanının kapsamı sadece ilgili endüstriyel kontrol sistemini işleten kuruluş ile sınırlı olmalıdır. Üreticinin şablon olarak hazırladığı ya da farklı ortamlarda kullandığı etki alanı yapıları kuruluş endüstriyel kontrol sistemleri içerisinde kullanılmamalıdır.
İSG-30	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, ortak erişime açık klasörler içerisindeki dosyalarda yüksek yetkili kullanıcı bilgileri gömülü olarak saklanmamalıdır.
İSG-31	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisine (domain controller) sadece gerekli protokoller üzerinden erişimi mümkün kılacak kısıtlamalar uygulanmalıdır.
İSG-32	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) üzerinde gerekli olmayan tüm ağ servisleri devre dışı bırakılmalıdır.

İSG-33	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) yedekli mimaride tasarlanmalıdır.
İSG-34	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı bileşenlerinde üretici tarafından sıkça kullanılan kullanıcı adı ve parolalar bulundurulmamalıdır.
İSG-35	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanı yöneticisi (domain controller) sunucusunun tekil görev için kullanılması sağlanmalıdır. DHCP, DNS ve dosya paylaşım vb. servisler için farklı sunucular konumlandırılmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
İSG-36	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanına ait tüm bileşenler yama yönetim politikalarına uygun olarak yönetilmelidir.
İSG-37	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan tüm bileşenler "Tehdit ve Zafiyet Yönetim" başlığına uygun olarak güvenlik denetimi ve sızma testlerine tabi tutulmalıdır. (İstemci, sunucu, konfigürasyon, GPO vb.) Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
İSG-38	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan sunucular için güvenli konfigürasyon kontrol listesi oluşturmalıdır.
İSG-39	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan sunucular oluşturulan güvenli konfigürasyon kontrol listesine göre periyodik gözden geçirilmelidir. Konfigürasyon değişikliklerini anlık olarak loglayacak yapılandırmalar devreye alınmalıdır.
İSG-40	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, etki alanında bulunan Grup İlkeleri (GPO) güvenli bir şekilde uygulanmalıdır.
İSG-41	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, yetkili hesapların parola özetlerinin çalınmasının engellenmesi için etki alanı yöneticisi (domain admin) hesabıyla endüstriyel operasyonlarda kullanılan istemci ve sunucularda gerekli olmadıkça işlem yapılmamalıdır. Operatör iş istasyonlarında parola özetleri tutulma sayısı 0 yapılmalıdır. Ayrıcalıklı kullanıcı hesapları Korunan Kullanıcılar (Protected Users) grubuna alınmalıdır.

İSG-42	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, aktif dizinde uzun süre kullanılmayan kullanıcı ve iş istasyonları tespit edilmelidir. Kullanılmayan kullanıcı ve iş istasyonları kuruluş politikalarına göre devre dışı bırakılmalıdır.
İSG-43	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, aktif dizin sorguları LDAP protokolü yerine güvenli LDAPs protokolü ile yapılacak şekilde konfigüre edilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
İSG-44	Endüstriyel İstemci ve Sunucu Güvenliği	OT Domain Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) etki alanı (domain) mimarisi kullanılması durumunda, yalnızca etki alanı yönetimini (Domain Controller) gerçekleştirmek için güvenli bir yönetici iş istasyonu konumlandırılmalı, ek yazılım veya rol yüklenmemeli, eposta, internet vb. erişimleri için kullanılmamalıdır.
İSG-45	Endüstriyel İstemci ve Sunucu Güvenliği	HMI Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS), operatörler günlük operasyonları gerçekleştirdikleri arayüzler (HMI) üzerinde operasyonu gerçekleştirmek için gerekli olan en düşük yetki ile çalışmalıdır. Arayüzler (HMI) yetki aşımına izin vermeyecek şekilde yapılandırılmalıdır.
İSG-46	Endüstriyel İstemci ve Sunucu Güvenliği	HMI Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerindeki (EKS), operatör istasyonlarının operatör arayüz yazılımını (HMI) devre dışı bırakarak bilgisayarın normal fonksiyonlarını kullanmasını engelleyebilecek şekilde yapılandırılmalıdır. İlgili uygulamalar sadece amaca uygun şekilde yetkilendirilmelidir. Bu yapılandırmalar "Tehdit ve Zafiyet Yönetim" başlığına uygun şekilde periyodik olarak test edilmelidir. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
İSG-47	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda kullanılacak sanallaştırma altyapısı kullanılıyorsa, bu altyapılar fiziksel olarak KBS ağlarında kullanılan sanallaştırma altyapılarından farklı olmalıdır.
İSG-48	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 3	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma sunucusunda kullanılan sanallaştırma yazılımı, güvenlik açığı barındırmayan en kararlı sürümde çalıştırılmalıdır.
İSG-49	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Ek kontrol	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma yazılımı ile beraber gelen güvenlik duvarı endüstriyel üretici gözetiminde aktif hale getirilmeli ve sadece ihtiyaç duyulan portlar üzerinden ihtiyaç duyulan IP adreslerine erişime izin vermelidir.
İSG-50	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma ünitelerine erişim sağlayabilen kullanıcıların, sanal makinelerin sahibi olan kullanıcıların ekranlarını yetkisiz olarak görüntülemesi engellenmelidir. Ayrıca yetkisiz konsol erişimleri de engellenmelidir. Her kullanıcı kimlik doğrulaması sonrasında erişim sağlanmalıdır.
İSG-51	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma ünitesinde kullanıcılar en az yetki prensibine uygun şekilde ilgili kullanıcı rollerine atanmalıdır.

İSG-52	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, ana bilgisayardan ve sanal makinelerden gerekli olmayan tüm hizmetler/donanımlar kaldırılmalıdır. Örneğin, kullanılmayan sanal donanımlar (sürücüler, ağ adaptörleri vb.) devre dışı bırakılmalıdır. Ayrıca gereksiz hipervizör hizmetleri (pano paylaşımı, dosya paylaşımı vb.) devre dışı bırakılmalıdır.
İSG-53	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanal disk küçültme (disk shrinking) işleminin sürekli olarak yapılması, sanal diskin kullanılamamasına ve veri kaybına sebebiyet verebileceği için bu ayarı yönetebilecek kullanıcılar belirlenerek, sadece bu kullanıcıların erişimine izin verilmelidir.
İSG-54	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma yazılımı çalıştığı tüm sunucularda merkezi olarak eş zamanlı güncellenmelidir.
İSG-55	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanal makineye ait diskler geri döndürülemez şekilde güvenli silme yöntemleri ile silinmelidir.
İSG-56	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, bellek paylaşımı (memory sharing) kullanılmıyor ise devre dışı bırakılmalıdır. Eğer bellek paylaşımı özelliği kullanılacak ise sanal makineler arasında endüstriyel katmanlı mimariye uygun gruptandırma gibi gerekli güvenlik önlemleri alınmalıdır.
İSG-57	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, gelecekteki ihtiyaçlar, yasal yükümlülükler ve olası güvenlik riskleri göz önünde bulundurularak sistem kaynaklarının planlaması yapılmalı ve kaynaklar sürekli izlenmelidir. Kapasite artırımı için kurumsal eşik değerleri tanımlanmalıdır.
İSG-58	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma ortamında kullanılmayan sanal makineler kapatılmalı, ağdan izole edilmeli ve sanal makine görev ömrünü tamamlayınca üzerinde yer alan veriler güvenli silme yöntemleri ile imha edilmelidir.
İSG-59	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, tüm sanal makine imajlarının bütünlüğünü denetleyecek ve izleyecek mekanizmalar devreye alınmalıdır.
İSG-60	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, ağ ortamları ve sanal makineler, kurum tarafından belirlenen kriterlere göre güvenilir ve güvenilmeyen bağlantılar arasındaki trafik kısıtlanacak şekilde yapılandırılmalıdır. Bu yapılandırmalar düzenli olarak gözden geçirilmelidir.
İSG-61	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, kontrol sistemi mimarisinde fiziksel olarak ayrı olması planlanan bileşenler sanal katmanda da izole edilmelidir. (DCS ve SIS sistemleri gibi)
İSG-62	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma sistemleri yönetim arayüzlerine erişim, iş ihtiyaçları doğrultusunda tanımlanan yetki ile güvenli bir şekilde yapılmalıdır.
İSG-63	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Ek kontrol	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanallaştırma ortamında kendinden imzalı sertifikalar yerine kuruma ait ve yetkili otoriteden alınmış sertifikalar kullanılmalıdır.

İSG-64	Endüstriyel İstemci ve Sunucu Güvenliği	OT Sanallaştırma Güvenliği	Seviye 2	Endüstriyel ağlarda sanallaştırma altyapısı kullanılıyorsa, sanal makineler arasındaki trafik güvenlik kontrollerinden geçirilmeli, olası zararlı trafiğin ağdaki diğer sanal ve fiziksel makinelere ulaşmaması için gerekli önlemler alınmalıdır.
İSG-65	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim tesisi bünyesinde kullanılan harici izleme sistemleri (GKC, RITM, Optimizasyon yazılımları, sektöre göre hava durumu izleme vb.) kapsamında kullanılan istemci ve sunucular en az elektrik üretim endüstriyel kontrol sistemleri (EKS) istemci ve sunucuları seviyesinde korunmalıdır.
İSG-66	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim tesisi bünyesinde kullanılan destek sistemleri (balance of plant, utilities, kömür alma, su alma vb.) kapsamında kullanılan istemci ve sunucular en az elektrik üretim endüstriyel kontrol sistemleri (EKS) istemci ve sunucuları seviyesinde korunmalıdır.
İSG-67	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim tesisi bünyesinde izleme amaçlı kullanılan BT odaklı istemci ve sunucular en az elektrik üretim endüstriyel kontrol sistemleri (EKS) istemci ve sunucuları seviyesinde korunmalıdır.
İSG-68	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim tesisi bünyesinde hibrit üretim veya birden fazla kontrol sistemi kullanılması durumunda, tüm endüstriyel kontrol sistemi istemci ve sunucuları bu başlık altında yer alan kontrol maddeleri ile uyumlu olmalıdır.
İSG-69	Endüstriyel İstemci ve Sunucu Güvenliği	Harici Sistemlerinin Güvenliği	Seviye 2	Elektrik üretim tesisi bünyesinde kullanılan kamu veya özel sektör entegrasyonları için konumlandırılan istemci ve sunucular elektrik üretim endüstriyel kontrol sistemleri (EKS) istemci ve sunucuları seviyesinde korunmalıdır.
İSG-70	Endüstriyel İstemci ve Sunucu Güvenliği	Endüstriyel Ağlarda Merkezi Yönetim	Seviye 1	Elektrik üretim operasyonları kapsamında aynı kuruluş bünyesinde farklı lisansa sahip santralleri merkezi olarak izleniyor veya yönetiliyorsa, merkezi operasyon noktasında kullanılan istemci ve sunucular "İstemci ve Sunucu Güvenliği" başlığı altındaki uygulanabilir tüm kontrolleri sağlamalıdır. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
İSG-71	Endüstriyel İstemci ve Sunucu Güvenliği	Endüstriyel Ağlarda Merkezi Yönetim	Seviye 2	Elektrik üretim operasyonları kapsamında aynı kuruluş bünyesinde farklı lisansa sahip santralleri merkezi olarak izlendiği veya yönetildiği durumda, merkezi operasyon noktasında aktif dizin (Domain) yapısı kullanılıyorsa her bir santral aktif dizin katmanında ayrıştırılmalıdır.

Endüstriyel Tehdit ve Zafiyet Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TZY-1	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi için gerekli bilgi kaynakları belirlenmelidir.
TZY-2	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi amacı ile belirlenen kaynaklardan siber güvenlik tehdit bilgisi toplanmalı ve işlenmelidir.
TZY-3	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinin (EKS) güvenliği ve sürekliliği için risk teşkil edebilecek tehditler belirlenmeli ve bu tehditlerin yönetimi için iyileştirme aksiyonları belirtilmelidir.
TZY-4	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin profillendirilmesi için tehdit hakkında en az aşağıdaki bilgiler edinilmelidir. -Tehdidin hedefi -Kabiliyetleri -Tehdit hedefinin endüstriyel operasyondaki önemi
TZY-5	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi için belirlenen bilgi kaynakları önceliklendirilmeli ve sürekli olarak takip edilmelidir.
TZY-6	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen tehditler analiz edilmeli, sınıflandırılmalı ve önceliklendirilmelidir.
TZY-7	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik zafiyetlerin yönetilebilmesi için gerekli bilgi kaynakları belirlenmelidir.
TZY-8	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik tehditlerin yönetilebilmesi amacı ile belirlenen kaynaklardan siber güvenlik zafiyet bilgisi toplanmalı ve işlenmelidir.
TZY-9	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinin (EKS) güvenliği ve sürekliliği için risk teşkil edebilecek zafiyetler belirlenmeli ve bu zafiyetlerin yönetimi için iyileştirme aksiyonları belirtilmelidir.
TZY-10	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	"Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddeleri doğrultusunda elektrik üretim endüstriyel kontrol sistemleri (EKS) için güvenlik analizleri ve testleri gerçekleştirilmelidir.
TZY-11	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen zafiyetler analiz edilmeli, sınıflandırılmalı ve önceliklendirilmelidir.
TZY-12	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) yönelik risk teşkil edebileceği değerlendirilen zafiyetler önceliklerine göre yönetilmelidir.

TZY-13	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine ait siber güvenlik yamaları "İstemci ve Sunucu Güvenliği" başlığına uygun olacak şekilde yamaların operasyonlara olan etkisi de gözden geçirilerek uygulanmalıdır. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
TZY-14	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetim yaklaşımı dokümente edilmiş olmalıdır.
TZY-15	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetim sürecinde ihtiyaç duyulabilecek tüm üçüncü taraflar belirlenmeli ve bu sürece dahil edilmelidir.
TZY-16	Endüstriyel Tehdit ve Zafiyet Yönetimi	Politika, prosedür, süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit ve zafiyet yönetimi için gerekli standart, kılavuz ve yasal mevzuatlar belirlenmelidir.
TZY-17	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin tehdit istihbaratı, bir bütün olarak izlenmelidir.
TZY-18	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Tehdit yönetimi kapsamında operasyonel güvenlik açısından arz güvenliğini riske atabilecek, doğal afetler, terör vb. gibi bilgiler de bütüncül bir yaklaşım sergileyecek şekilde değerlendirilmelidir.
TZY-19	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin yerel ve küresel tehdit istihbarat kaynakları bir bütün olarak yönetilmelidir. (Bu kaynaklar üretici sayfaları, küresel bilgilendirme sayfaları gibi kaynaklar olabilir.)
TZY-20	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit istihbaratı yönetimi	Seviye 2	Tehdit istihbarat kaynakları KBS ve EKS bileşenlerine ilişkin tehditleri kapsamalıdır.
TZY-21	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit tespiti	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin tehditler (saldırgan aktiviteleri) gerçek zamanlı olarak izlenebilmelidir. Bu izleme, istemci ve sunucu üzerinden bilgi toplanarak veya ağ trafiği takip edilerek gerçekleştirilebilir.
TZY-22	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel tehdit tespiti	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin bir saldırı tespiti yapılması durumunda, söz konusu saldırılar sınıflandırılmalıdır. (operasyonel tehditler, siber güvenlik tehditleri, fiziksel, ağ tehditleri vb.)
TZY-23	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizi "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine göre aktif veya pasif yöntemlerle (manuel ya da otomatize araçlarla) en az yılda bir kez gerçekleştirilebilir durumda olmalıdır.

TZY-24	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizi "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine uygun yöntemlerle gerçekleştirilmeli ve en az aşağıda belirtilen bileşenleri kapsamalıdır. - İş istasyonu - İnsan Makine arayüzü (HMI) iş istasyonu - Sunucu tabanlı riskler (DCS, SCADA, OPC, Historian vb.) - Endüstriyel yazılım uygulamaları (DCS, SCADA yazılımları) - Siber güvenlik uygulama ve çözümleri - Mühendislik iş istasyonu - Endüstriyel ağ ve ekipmanları - Endüstriyel altyapı kontrol katmanı ekipmanları (PLC, RTU, Röle/IED, Safety/Emniyet sistemleri) - Sayaçlar - KBS ağları entegrasyon bileşenleri (Üretim İzleme vb.) - Destek sistemleri, (Utilities, balance of plant), izleme sistemleri (GKC, RITM vb.), kontrol sistemleri ile entegre olan diğer sistemler
TZY-25	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizleri farklı kaynakları girdi olarak kullanılmalıdır. (Sızma testleri, güvenlik testleri, analizleri, zafiyet taramaları vb.)
TZY-26	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet analizleri için otomatize bir araç kullanılacaksa seçilen aracın teknolojisi, protokol desteği ilgili altyapıya uygun olmalıdır.
TZY-27	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin siber güvenlik zafiyetleri bir yaşam döngüsü şeklinde yönetilmelidir. (Tespit, iyileştirme, doğrulama, kapatma, kabul vb.)
TZY-28	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin tespit edilen her bir siber güvenlik zafiyeti için ilgili birim ve personellere sorumluluk ataması gerçekleştirilmelidir.
TZY-29	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin risk analizi, sızma testi, güvenlik analizi çıktılarının eğilimi sürekli olarak izlenmelidir.
TZY-30	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri tüm endüstriyel bileşenlerini içermelidir. (Elektrik üretim kontrol sistemleri, safety/emniyet sistemleri, destek sistemleri vb.)
TZY-31	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri katmanlı mimaride yer alan tüm katmanlarda uygulanmalıdır.
TZY-32	Endüstriyel Tehdit ve Zafiyet Yönetimi	Endüstriyel zafiyet yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ilişkin zafiyet yönetimi faaliyetleri, EKS varlıklarının sürüm bilgisinden zafiyet tespitine imkan vermelidir. Bu amaçla manuel veya otomatize araçlar kullanılabilir.

Endüstriyel Siber Güvenlik Risk Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
ERY-1	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi Stratejisi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemleri (EKS) için dokümante edilmiş bir endüstriyel siber güvenlik risk yönetimi stratejisi olmalıdır. Risk yönetim metodolojisi endüstriyel altyapılar için özelleştirilmiş olmalıdır.
ERY-2	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi Stratejisi	Seviye 1	Endüstriyel siber güvenlik risk yönetim stratejisi, endüstriyel operasyonlara etkinin dikkate alınması da dahil olmak üzere, risk önceliklendirmesi için bir yaklaşıma sahip olmalıdır. Bu strateji endüstriyel operasyonlar dikkate alınarak hazırlanmalıdır.
ERY-3	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Belirlenen riskler, risk azaltma, risk kabulü, riskten kaçınma veya riskin transferi işlemleri çerçevesinde yönetilmelidir. Bu sürece ilişkin gerekli dokümantasyon oluşturulmalı ve bu dokümanlar üç yıl süreyle saklanmalıdır.
ERY-4	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme dokümanı asgari olarak, “risk numarası, risk kategorisi, riskin oluşması için koşullar, zafiyet, tehdit, risk, riski taşıyan bileşen/bileşen grubu, riskten etkilenen bileşen/bileşen grubu, riskin etki değeri, riskin gerçekleşme olasılığı” başlıklarını içermelidir.
ERY-5	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme dokümanı, endüstriyel operasyonlarda veya bilgi teknolojileri sistemlerinde (yeni tehdit ve zafiyetler belirlendiği durumlar dahil olmak üzere) önemli değişiklikler olduğunda veya sistemin güvenlik durumunu etkileyebilecek diğer koşullar oluştuğunda güncellenmelidir.
ERY-6	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk gerçekleşme olasılığı en az “normal, yüksek ya da çok yüksek” dereceleri kullanılarak değerlendirilmelidir.
ERY-7	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk işleme planları, risklerin azaltılmasına ilişkin uygulanması veya alınması gereken önlem ve kontrolleri içermelidir.
ERY-8	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Tespit edilen riskler analiz edilerek, risk yönetimi stratejisine uygun olarak işleme faaliyetleri önceliklendirilmelidir.
ERY-9	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Tespit edilen riskler, risk yönetimi stratejisine uygun olarak izlenmelidir.
ERY-10	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk analizi sonuçları, ağ (KBS ve/veya EKS) mimarisine ait risk değerlendirme sonuçlarını da içermelidir. Risk analizlerinde mimari hatalar ve zafiyetler de girdi olarak kullanılmalıdır.

ERY-11	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Endüstriyel siber güvenlik risk yönetimi faaliyetleri için oluşturulan dokümanlar düzenli olarak takip edilmelidir. (Strateji dokümanları, politika ve prosedürler, formlar vb.)
ERY-12	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetleri için paydaşlar belirlenmeli ve risk yönetimi sürecine dahil edilmelidir.
ERY-13	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetlerini desteklemek için yeterli kaynak (insan kaynağı, finansman vb.) sağlanmalıdır.
ERY-14	Endüstriyel Siber Güvenlik Risk Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Risk yönetimi faaliyetlerinin içeriğinde yer alacak standartlar ve/veya kılavuzlar belirlenmelidir. (NIST 800-53, NIST800-82, ISA 62443, ISO 27019, C2M2 vb.)
ERY-15	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi nitel ve nicel olarak ölçüme olanak tanınmalıdır.
ERY-16	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi risk kabul kriterlerini ve risk kabul değerini tanımlamalıdır.
ERY-17	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi risk sahibini tanımlamalıdır. Riskler ilgili risk sahibine atanmalıdır.
ERY-18	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Endüstriyel siber güvenlik risk belirleme sürecinde endüstriyel operasyonlara etkiye göre derecelendirme yapılmalıdır.
ERY-19	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim metodolojisi tekrar edilebilir, karşılaştırılabilir ve tutarlı sonuçlar üretebilir olmalıdır.
ERY-20	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, tüm elektrik üretim proseslerini (elektrik üretim prosesleri, destekleyici prosesler) ve elektrik üretim endüstriyel kontrol sistemi bileşenlerini içermelidir. (İstemci/sunucu, PLC, RTU vb.)
ERY-21	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri, elektrik üretim işlemlerinin gerçekleştirildiği yerleşkeye ilişkin fiziksel güvenlik risklerini içermelidir.
ERY-22	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim faaliyetleri endüstriyel iletişim protokollerini içermelidir.
ERY-23	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk Yönetim faaliyetleri entegrasyon güvenliği ve ağ güvenlik risklerini içermelidir.

ERY-24	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetimi faaliyetlerinde, "Enerji Sektöründe EKS Güvenlik Kontrolleri" başlıkları en az aşağıdaki bileşenler için uygulanmalıdır. - İş istasyonu riskleri - İnsan Makine arayüzü (HMI) iş istasyonu riskleri - Sunucu tabanlı riskler (DCS, SCADA, OPC, Historian vb.) - Endüstriyel yazılım uygulamaları riskleri (DCS, SCADA yazılımları) - Siber güvenlik uygulama ve çözümleri - Mühendislik iş istasyonu riskleri - Endüstriyel ağ ve ekipmanları güvenlik riskleri - Endüstriyel altyapı kontrol katmanı ekipmanları güvenlik riskleri (PLC, RTU, Röle/IED, Safety/Emniyet sistemleri) - Sayaçlara ilişkin güvenlik riskleri - KBS ağları entegrasyon riskleri (Üretim İzleme vb.) - Destek sistemleri, (Utilities, balance of plant), izleme sistemleri (GKC, RITM vb.), kontrol sistemleri ile entegre olan diğer sistemler
ERY-25	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetimi üçüncü taraf bilgi güvenliği risklerini içermelidir.
ERY-26	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci ISO 27001 BGYS ve CB-DDO formlarına uygun olarak işletilmelidir.
ERY-27	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci kapsamında artık risk yönetim ilkeleri tanımlanmalıdır. Risk işleme sonrası kalan artık riskler; risk sahibi ve üst yönetim tarafından onaylanmalıdır.
ERY-28	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci, operasyonel süreklilik risklerini içermelidir.
ERY-29	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Siber güvenlik riskleri ethernet ve seri iletişim tabanlı saldırı vektörleri dikkate alınarak belirlenmelidir.
ERY-30	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim sürecinde; sızma testleri, güvenlik analizleri, iç denetim çıktıları da girdi olarak kullanılmalıdır.
ERY-31	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme sürecinde her bir endüstriyel siber güvenlik riskinin, çevre etkisi, finansal etkisi ve insana etkisi belirlenmelidir.
ERY-32	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk değerlendirme sürecinde her bir endüstriyel siber güvenlik riskinin diğer kritik altyapılara olan etkisi de değerlendirilmelidir. (ulaşım, enerji, kritik kamu kurumları (savunma sanayi vb.), sanayi üretimi)

ERY-33	Endüstriyel Siber Güvenlik Risk Yönetimi	Endüstriyel Siber Güvenlik Risk Yönetimi	Seviye 1	Risk yönetim süreci insan temelli riskleri de içermelidir. (Personel, operatör, mühendis, KBS çalışanı, siber güvenlik çalışanı, üretici ve alt yüklenici çalışanları)
--------	--	--	----------	--

Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
VKY-1	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları için envanter oluşturulmalıdır. Envanter Yönetimi amaca özel olarak oluşturulmalıdır.
VKY-2	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	Bu envanter, siber saldırı hedefi olabilecek her türlü bileşeni de içermelidir. (Yazıcı, IoT Cihazlar, kartlı geçiş sistemi vb.)
VKY-3	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları envanteri, siber güvenlik süreçlerini destekleyen öz nitelikler içermelidir. (Konum, varlık önceliği, işletim sistemi ve donanım yazılımı sürümleri vb.) Envanterdeki KBS ve EKS varlıklarına, bilgi varlıklarının fonksiyon ve görev önemine göre tanımlanmış CB DDO kriterlerini de göz önünde bulundurarak öncelik verilmelidir.
VKY-4	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları için oluşturulan envanter periyodik olarak ve sistem değişikliği durumunda güncellenmelidir.
VKY-5	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 2	EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) ve bilgi varlıkları envanteri, varlık kullanım ömrü (end-of-life) ve üretici desteğinin sonlanması (end-of-support) gibi bilgileri içermelidir.
VKY-6	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	EKS Varlık Yönetimi	Seviye 1	Envanterde kullanım ömrü sonuna gelmiş veya değişimi yapılacak olan KBS ve EKS varlıklarına ait veriler güvenli bir şekilde silinmelidir.
VKY-7	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Bilgi Varlığı Envanteri Yönetimi	Seviye 2	Elektrik üretim endüstriyel proseslerinin devamlılığı için önemli olan bilgi varlıklarının envanteri oluşturulmalıdır. (Bu bilgi varlıkları, analog komutlar, özel konfigürasyon parametreleri olabilir) Envanter yönetimi endüstriyel prosese özel olmalıdır.
VKY-8	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 1	Temel konfigürasyon mimarisi oluşturulmalıdır. Konfigürasyonlarda siber güvenlik açısından gerekli olan minimum isterler dokümanite edilmelidir. (IP adresleri, parolalar, servis/port, kritik set değerleri vb.)
VKY-9	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 2	Temel konfigürasyon mimarisi, varlıklara konfigürasyon dağıtımı ve geri yükleme süreçlerinde kullanılmalıdır.
VKY-10	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 2	Yeni gerçekleştirilen varlık konfigürasyonlarının, temel konfigürasyon mimarisine göre tutarlılıkları izlenmelidir.

VKY-11	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Konfigürasyon Yönetimi	Seviye 1	Temel konfigürasyon mimarisi, periyodik olarak, sistem değişiklikleri ve siber güvenlik mimarisindeki değişikliklere göre gözden geçirilmeli ve güncellenmelidir.
VKY-12	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Varlıklarda yapılacak değişiklikler, uygulanmadan önce, kurum tarafından tanımlanmış ve dokümente edilmiş olan sistem etkisi ve siber güvenlik isterlerine göre değerlendirilmeli, test edilmeli ve onaylanmalıdır. Bu testler siber güvenlik gereksinimlerini karşılamalıdır. Değişikliklere ilişkin kayıtlar tutulmalıdır.
VKY-13	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Değişim yönetimi takibi, varlıkların tüm yaşam döngüsünü ele almalıdır. (Satın alma, dağıtım, operasyon, kullanımdan kaldırılması vb.)
VKY-14	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Varlık Değişikliklerinin Yönetimi	Seviye 1	Değişiklik kayıtları, varlıkların siber güvenlik gereksinimlerini etkileyen değişikliklerle ilgili bilgileri de içermelidir.
VKY-15	Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Varlık yönetim sürecinde dokümente edilmiş prosedürler oluşturulmalıdır. İlgili prosedüreler takip edilmeli ve sürdürülmelidir. Varlık yönetim sürecinde gerekli üst yönetim desteği sağlanmalıdır. Süreçten sorumlu personeller atanmalı ve gerekli yetkilendirilmeler yapılmalıdır. Varlık yönetim sürecinin etkinliği değerlendirilmeli ve izlenmelidir.

Endüstriyel Kimlik ve Erişim Yönetimi

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
KEY-1	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan operatör iş istasyonlarında, sunucularda, mühendislik iş istasyonlarında, uygulamalarda ve ağ cihazlarında tahmin edilebilir ya da basit kullanıcı adı/parola kullanılmamalıdır. Sistem tarafından karmaşık parola atamaları zorlanmalıdır.
KEY-2	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan operatör iş istasyonlarında, sunucularda, mühendislik iş istasyonlarında, uygulamalarda ve ağ cihazlarında alt yükleniciler tarafından farklı tesislerde aynı kullanıcı ve parola kullanılmamalıdır.
KEY-3	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan bileşenlerde operatör yetkisi ve mühendislik yetkisi ayrıştırılmalıdır.
KEY-4	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Ek Kontrol	Elektrik üretim endüstriyel kontrol sistemi (EKS) uygulamalarında (DCS, SCADA) operatörlerin yaptıkları işlemlere göre yetki ayrıştırması yapılmalıdır.
KEY-5	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) uygulamalarına (DCS, SCADA) ait kullanıcı ve yetkilendirme dosyaları, kullanıcıların erişebildiği alanlarda saklanmamalıdır. Bu tür dosyalara erişimler kısıtlanmalıdır.
KEY-6	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Ek Kontrol	Elektrik üretim endüstriyel kontrol sisteminde (EKS) işletim sistemi kullanıcılarıyla endüstriyel uygulama (DCS, SCADA) kullanıcıları birbirinden ayrıştırılmalıdır.
KEY-7	Endüstriyel Kimlik ve Erişim Yönetimi	Hesap Yönetimi	Ek Kontrol	Elektrik üretim endüstriyel kontrol sistemi (EKS) operatör kullanıcılarına ait hesaplar tekil kullanıcı esasına göre oluşturulmalıdır.
KEY-8	Endüstriyel Kimlik ve Erişim Yönetimi	Hesap Yönetimi	Seviye 1	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine ait kullanıcı adı ve parolalar ilgili sistemden farklı bir dijital ortamda ya da fiziksel olarak saklanmamalıdır. (Dosya sunucusu, excel dosyaları, kağıt ve panolarda saklama vb.)
KEY-9	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sisteminde (EKS) gerçekleştirilecek kontrol işlemleri (yüksek yetkili operasyonel işlemler vb.) için ikinci bir onay mekanizması kurgulanmalıdır.
KEY-10	Endüstriyel Kimlik ve Erişim Yönetimi	Erişim ve Yetki Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) uygulamalarında (DCS, SCADA) mevcut kullanıcıdan farklı bir kullanıcı ya da yetkiye geçiş yapılırken parola doğrulaması yapılmalıdır.

KEY-11	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) uygulamalarına (DCS, SCADA) ait parola bilgileri tersine mühendislik ile elde edilemeyecek şekilde oluşturulmalıdır.
KEY-12	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için kullanılacak kullanıcı adı ve parolalar, endüstriyel bileşenlere ait kullanıcı adı ve parolalardan farklı olmalıdır.
KEY-13	Endüstriyel Kimlik ve Erişim Yönetimi	Parola Yönetimi	Seviye 2	KBS altyapılarında kullanılan ve elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine entegrasyonu olan sistem ve uygulamalara ait kullanıcı adı ve parolalar, endüstriyel bileşenler üzerinde tanımlı kullanıcı adı ve parolalardan farklı olmalıdır.
KEY-14	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda iki faktörlü kimlik doğrulama mekanizmaları devreye alınmalıdır.
KEY-15	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda uzak erişim sağlayan her bir kullanıcıya özel kullanıcı adı ve parola bilgisi atanmalıdır.
KEY-16	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için kullanılacak hesaplar geçici süre ile oluşturulmalıdır.
KEY-17	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda erişime ilişkin tüm kayıtlar saklanmalıdır. (Erişim talebi, erişim onayı, erişim sırasında oluşan sistem kayıtları vb.)
KEY-18	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim için bir atlama noktası (jump box) kullanılıyorsa ilgili bileşen üzerinde bulunan hesapların ele geçirilmesini önlemek amacıyla gerekli sıkılaştırmalar devreye alınmalıdır.
KEY-19	Endüstriyel Kimlik ve Erişim Yönetimi	Uzak Erişim Hesap Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemi (EKS) bileşenlerine uzaktan erişim sağlanması durumunda, uzak erişimin sadece izin verilen bileşen ve sisteme yapılmasını garanti altına alacak ağ ve sistem tabanlı erişim kısıtlamaları uygulanmalıdır.

Endüstriyel Olay Yönetimi ve Süreklilik

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
OYS-1	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale politika ve prosedürleri, elektrik üretim endüstriyel kontrol sistemlerini (EKS) kapsayacak şekilde hazırlanmalıdır.
OYS-2	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Kurumsal SOME rehberinde adreslendiği şekilde kurum içi rol ve sorumluluklara uygun olarak olay müdahale eğitimleri alınmalıdır.
OYS-3	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale eğitimleri siber güvenlik kaynaklı olarak oluşabilecek kriz yönetimini de içermelidir.
OYS-4	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale eğitimleri elektrik üretim endüstriyel kontrol sistemlerinde (EKS) siber güvenlik kaynaklı olarak oluşabilecek "görünürlük kaybı" ve "kontrol kaybı" etkilerine sahip senaryoları içermelidir.
OYS-5	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Kuruluş, olay müdahale testleri kapsamında, kendi yetkinliklerini belirli periyotlarla simülasyonlar aracılığı ile test etmelidir.
OYS-6	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale testleri, iş sürekliliği, acil durum yönetimi, kriz yönetimi gibi süreç ve planlarla koordine olarak gerçekleştirilmelidir.
OYS-7	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale testleri kapsamında performans ölçümleri gerçekleştirilmelidir. (Ekip performansı, sistem yeterlilikleri, testlerin uygunluğu, birimler arası koordinasyon yeteneği vb.)
OYS-8	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale için gerekli yöntemler tanımlanmalı ve uygulanmalıdır. (Log toplama, ağ trafiği toplama, adli bilişim verisi toplama vb.)
OYS-9	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Ek kontrol	Olay müdahale kapsamında olaylara otomatik cevap verme süreçleri tanımlanmalıdır. (Route ekleme çıkarma, kural ekleme çıkarma vb.)
OYS-10	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale kapsamında, endüstriyel operasyonların sürekliliğine ilişkin senaryolar tanımlanmalıdır. (Manuel operasyona geçiş, yedek kontrol merkezine geçiş vb.)
OYS-11	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 2	Olay müdahale yaklaşımı iç tehditlerin (çalışanlar, ağa erişim yetkisi olan alt yükleniciler ve üreticiler vb.) tespitini içerecek şekilde tasarlanmalıdır.
OYS-12	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale kapsamında, kurum içi birimlerin koordinasyonu tanımlanmalıdır. (İK, İşletme Birimleri, Hukuk vb.) Her bir olay için bilgi verilen, raporlanan, sorumlu kişi/birim şeklinde sınıflandırmalar yapılmalıdır.
OYS-13	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ve sonrasında, kurum dışı otoritelerle iletişim ve koordinasyon gereklilikleri tanımlanmalıdır.

OYS-14	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ve sonrasında, gerek duyulması halinde kuruluşa hizmet veren alt yüklenici ve üreticilerle gerçekleştirilecek koordinasyon süreci tanımlanmalıdır.
OYS-15	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale ekibi, Kurumsal SOME yönergeleri kapsamında oluşturulmalıdır.
OYS-16	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Tüm olay müdahale süreçleri Kurumsal SOME Rehberine uyumlu olmalıdır.
OYS-17	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale süreçleri, zararlı yazılım analizi ve adli bilişim analizini kapsamalıdır.
OYS-18	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 3	Olay müdahale kapsamında, kurum anormal durum tespit yeteneklerine sahip olmalıdır. Kurumlar bunu sağlamak için istemci/sunucu, uygulama veya ağ tabanlı bir çözüm kullanabilir.
OYS-19	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay müdahale süreçleri, medya ve ilgili otoritelerle (elektrik iletim şebekesi, düzenleyici kurum vb.) iletişimlerini içermelidir.
OYS-20	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale ve Cevap Verme	Seviye 1	Olay yönetimi süreci, elektrik üretim operasyonlarına özel endüstriyel proses, varlık ve ekipmanlara uyumlu şekilde tanımlanmalıdır.
OYS-21	Endüstriyel Olay Yönetimi ve Süreklilik	Olay İzleme	Seviye 2	Olay izleme süreçleri elektrik üretim endüstriyel kontrol sistemleri (EKS) için de devreye alınmalıdır.
OYS-22	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Raporlama	Seviye 1	Olay raporlama süreçleri Kurumsal SOME rehberine uyumlu olmalıdır.
OYS-23	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Raporlama	Seviye 1	Olay raporlama süreçleri, olayın yaşanmasına neden olan zafiyetlerin bilgisini içermelidir.

OYS-24	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Müdahale Planı	Seviye 1	Kurum kendine özgü olay müdahale planlarını geliştirmelidir. Bu planlar en az aşağıdaki başlıkları içermelidir. - Olay müdahale organizasyonu (Roller ve görevler) - Olay tanımı (Olay sınıflandırma) - Raporlama (Olay bildirimi, analizi) - Kaynakların sağlanması - Bilgi paylaşımı (Kurum ve kurum dışı iletişim esasları) - Doküman yönetimi (Doküman güncelleme ve dağıtımı) - Kök neden analizi (Olayların kök neden analiz yöntemi ve raporlaması. Üçüncü taraflarda meydana gelebilecek olayların kök neden analizi hususuna sözleşmelerde yer verilmelidir.) - Olaylardan alınan dersler (lessons learned) ve olayların tekrarlanmasının engellenmesi - Olay müdahale simülasyonu ve başarı performans ölçümü
OYS-25	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 1	Tespit edilen olaylar belirli bir rol ya da kişiye atanmalıdır.
OYS-26	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 1	Olay tespiti için kriterler belirlenmelidir. (Olay tanımı, nereye bakılacağı vb.)
OYS-27	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan ağ ve güvenlik cihazları log üretme kapasitesine sahip olmalıdır.
OYS-28	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan ağ ve güvenlik cihazları log yönlendirme kapasitesine sahip olmalıdır.
OYS-29	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan ağ ve güvenlik cihazları log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-30	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan ağ ve güvenlik cihazlarına ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-31	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Seviye-2 ve üzeri katmanlarda (Purdue modeline göre) bulunan ağ cihazlarına ilişkin loglar merkezi olarak toplanmalı ve işlenmelidir.
OYS-32	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan endüstriyel cihazlar (PLC, Safety PLC, RTU, IED, Röle) log üretme kapasitesine sahip olmalıdır.

OYS-33	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Alarm ve Log Yönetimi	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan endüstriyel cihazlar (PLC, Safety PLC, RTU) log yönlendirme kapasitesine sahip olmalıdır.
OYS-34	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Alarm ve Log Yönetimi	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan endüstriyel cihazlar (PLC, Safety PLC, RTU, IED, Röle) log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-35	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan yazılım ve uygulamalar (DCS, SCADA, veri toplama vb.) log üretme kapasitesine sahip olmalıdır.
OYS-36	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan yazılım ve uygulamalar (DCS, SCADA, veri toplama vb.) log yönlendirme kapasitesine sahip olmalıdır.
OYS-37	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan yazılım ve uygulamalar (DCS, SCADA, veri toplama vb.) log derecelendirme veya sınıflandırma kapasitesine sahip olmalıdır.
OYS-38	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde bulunan yazılım ve uygulamalar (DCS, SCADA, veri toplama vb.) ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-39	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan akıllı/endüstriyel sayaçlar log tutma, yönlendirme, derecelendirme ve sınıflandırma kapasitesine sahip olmalıdır.
OYS-40	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan akıllı/endüstriyel sayaçlara ilişkin loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-41	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Olay yönetimi gerçekleştirebilmek için kullanılan tüm log kaynakları aynı saat dilimi üzerinden senkronize edilmelidir.

OYS-42	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucularda aşağıdaki tipteki loglar tutulmalıdır. - İşletim sistemi logları - Bileşen üzerindeki güvenlik yazılımları logları (kötü amaçlı yazılım koruma uygulamaları, whitelisting uygulamaları) - Bileşen üzerinde bulunan diğer yazılımlara ilişkin loglar
OYS-43	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucular log yönlendirme kapasitesine sahip olmalıdır.
OYS-44	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucular log derecelendirme ve sınıflandırma kapasitesine sahip olmalıdır.
OYS-45	Endüstriyel Olay Yönetimi ve Süreklilik	Endüstriyel Siber Güvenlik Log Yönetimi	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucularda kayıt altına alınan loglar merkezi olarak toplanmalı, işlenmeli ve anlamlandırılmalıdır.
OYS-46	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Tespit Etme	Seviye 2	Olay tespit yetenekleri, tehdit, zafiyet ve risk yönetim süreçleri ile bütünleşik olmalıdır.
OYS-47	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Hangi olayların USOM'a bildirileceğine dair ilişkin kriter tanımlanmalıdır. (operasyonların etkilenmesi, hizmet verememe, endüstriyel operasyonlara etki ve etkilerin dereceleri vb.) Olay bildirim kriteri belirli periyotlarla gözden geçirilmeli ve gerekli durumlarda güncellenmelidir.
OYS-48	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) gerçekleşen siber güvenlik bildirimleri sürekli izlenerek ve analiz edilerek olay bildirim sürecinde girdi olarak kullanılabilir.
OYS-49	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Siber güvenlik bildirimlerinin siber güvenlik olayı olup olmadığına karar vermek için kriterler belirlenmelidir.
OYS-50	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olaylarını Analiz Etme ve Bildirme	Seviye 1	Olayların yaşam döngüsü uçtan uca takip edilmelidir. (Kime atandığı, nasıl çözüldüğü, kimin çözdüğü vb.)
OYS-51	Endüstriyel Olay Yönetimi ve Süreklilik	Olay Yönetiminde İş Sürekliliği	Seviye 1	Belirli olay ve bildirimlerin yaşanması durumunda kullanılacak iş sürekliliği planları geliştirilmelidir. (Hizmet kesintisi, operasyonel arıza vb.)
OYS-52	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) bulunan tüm ağ ve güvenlik cihazlarının konfigürasyonları periyodik olarak alınmalı, güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.

OYS-53	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) bulunan tüm endüstriyel ekipman, uygulama ve bileşenlerin lojik ve/veya konfigürasyonları periyodik olarak yedeklenmeli, yedekler güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.
OYS-54	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) bulunan istemci ve sunucuların imaj ve veri yedekleri periyodik olarak alınmalı, güvenli şekilde saklanmalı ve periyodik geri dönüş testleri gerçekleştirilmelidir.
OYS-55	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) iş sürekliliği planları hazırlanırken olası olayların etkileri girdi olarak kullanılmalıdır. (Hizmet kesintisi, görüntü kaybı, kontrol kaybı, üretim kaybı vb.)
OYS-56	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) operasyonların devamlılığı için gerekli olan varlık ve süreçler iş sürekliliği planına dahil edilmelidir.
OYS-57	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planları periyodik olarak test edilmeli ve gerekli durumlarda güncellenmelidir.
OYS-58	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Alınan veri, imaj konfigürasyon/lojik yedekleri orijinal veri seviyesinde korunmalıdır.
OYS-59	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Alınan tüm yedekler, mantıksal ve fiziksel olarak orijinal verilerden ayrıştırılmalıdır.
OYS-60	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Operasyon açısından önem arz eden varlıklar için kurtarma süresi hedefleri (RTO) ve kurtarma noktası hedefleri (RPO) süreklilik planlarına dahil edilmelidir.
OYS-61	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planlarının ne zaman devreye alınacağına dair kriter tanımlanmalıdır.
OYS-62	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Hazırlanan süreklilik planı, tehdit, zafiyet ve risk yönetim süreçleri ile bütünleşik olarak işletilmelidir.
OYS-63	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Seviye 1	Süreklilik planının testleri ya da icrası sonucu oluşan sonuçlar plan ile karşılaştırmalı gerekli durumlarda güncellenmelidir.
OYS-64	Endüstriyel Olay Yönetimi ve Süreklilik	Siber Güvenlik Olay Yönetimi ve İş Sürekliliği	Ek kontrol	(Ülkemizin yer aldığı coğrafyada yaşanan ve yaşanması olası doğal afetler göz önünde bulundurulduğunda) Kuruluşlar, ISO 22301 standardına sahip olmalıdır.

OYS-65	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden tüm kritik bileşenler yedekli yapıda olmalıdır. (Ağ ve güvenlik cihazları, sunucular, mühendislik iş istasyonları, kritik endüstriyel ekipmanlar vb.)
OYS-66	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Seviye 3	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden ağ bileşenleri için en az 1 adet olacak şekilde soğuk yedek (cold backup) tutulmalıdır. (Switch, router vb.)
OYS-67	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden güvenlik bileşenleri için en az bir adet soğuk yedek tutulmalıdır. (Güvenlik duvarı, IPS vb.)
OYS-68	Endüstriyel Olay Yönetimi ve Süreklilik	Yedekleme ve Yedeklilik	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonun sürekliliği için önem arz eden supervisory katmanda yer alan sunucu/istemci için en az bir adet soğuk yedek tutulmalıdır.
OYS-69	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kurum, kurumsal misyon, iş süreci veya sistem düzeyinde tanımlanan acil durum planlama politikası; amaç, kapsam, roller, sorumluluklar, yönetim desteği, kurumsal varlıklar arasındaki koordinasyon ve uyumluluğu ele almalıdır. Acil durum planlama politikası; kurumun diğer politika ve prosedürleri ile uyumlu olmalıdır.
OYS-70	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Mevcut acil durum planı, politika ve prosedürleri Kurum tarafından tanımlanan olay veya zaman periyotlarına göre gözden geçirilmeli ve güncellenmelidir.
OYS-71	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planlarında ilgili kişi ve birimlerin iletişim bilgileri yer almalıdır.
OYS-72	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, bir sistem kesintisinde, siber saldırı veya arıza durumlarına rağmen işletmenin misyon ve fonksiyonlarını sürdürmeyi ele almalıdır.
OYS-73	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planı, yetkisiz ifşa ve içeriğinin değiştirilmesine karşı korunmalıdır.
OYS-74	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planı, normal operasyonlara dönüş planlarını içermelidir.
OYS-75	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum gereksinimlerini sağlamak için acil durum planı, harici hizmet sağlayıcıların acil durum planlarıyla koordine edilmelidir.
OYS-76	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kriz durumlarında personelin etkin müdahalesini kolaylaştırmak için acil durum eğitimleri periyodik olarak düzenlenmelidir.

OYS-77	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, simülasyon ortamlarında test edilmelidir.
OYS-78	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Acil durum planları, bölge çapında genel bir hizmet kesintisi veya felaket durumunda planların çalıştırılabilmesi için gerekli önlemleri içermelidir.
OYS-79	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Süreklilik gereksinimlerine uygun olarak kritik hizmet sağlayıcılar yedeklenmelidir. (Enerji, su vb.)
OYS-80	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Seviye 2	Kuruluşlar, hizmet sağlayıcılardan acil durum planlarını oluşturmalarını istemelidir. Hizmet sağlayıcıların acil durum planları periyodik olarak gözden geçirilmelidir.
OYS-81	Endüstriyel Olay Yönetimi ve Süreklilik	Acil Durum Yönetimi	Ek kontrol	Acil durum testleri kapsamında tüm yedeklilik senaryoları test edilmelidir.

Akıllı Cihaz Güvenliği

No	Ana kontrol	Alt Kontrol	Seviye	Kontrol
ACG-1	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan tüm bileşenlerin ve iletişim cihazlarının bir envanteri oluşturulmalıdır.
ACG-2	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan tüm bileşenler "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları"nın ilgili maddelerine uygun şekilde periyodik olarak güvenlik testlerine tabi tutulmalıdır.
ACG-3	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan tüm bileşenler risk yönetim süreci içerisinde değerlendirilmelidir.
ACG-4	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısı içerisinde gömülü yazılıma (firmware) sahip bileşenler için güvenli yapılandırma kontrol listesi hazırlanmalı ve işletme için minimum güvenlik kontrolleri belirlenmelidir. (Örnek referans: https://www.opencompute.org/documents/csis-firmware-security-best-practices-position-paper-version-1-0-pdf)
ACG-5	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısı içerisinde bulunan cihazlar üzerindeki debug arayüzleri (JTAG, SWD) devre dışı bırakılmalı veya uygun yetkilendirme yöntemleri ile aktif edilebilmelidir. (JTAG Enabling, SWD authentication vb.) <i>Bunun sağlanamadığı durumlarda ilgili bileşenlere fiziksel erişimler kısıtlanmalıdır.</i>
ACG-6	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısı içerisinde bulunan cihazlarda code Integrity/kod bütünlük koruma mekanizmaları sahaya konumlandırılmadan önce devreye alınmalı ve bu durumun korunması sağlanmalıdır. (Secure boot, boot konfigürasyonlarının devre dışı bırakılması vb.) <i>Bunun sağlanamadığı durumlarda ilgili bileşenlere fiziksel erişimler kısıtlanmalıdır.</i>

ACG-7	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Ek kontrol	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaçlar üzerinde kritik parametrelerin saklanması, cihaz kimliğinin değiştirilemez şekilde eşsiz bir anahtar ile ayırt edilebilmesi ve trust anchor (Root of Trust) amacıyla SE (Secure Element), HSM (Hardware Security Module), TPM (Trusted Platform Module), TEE (Trusted Execution Environment - ARM Trustzone) gibi bileşenler akıllı cihaz tarafından kullanılmalıdır.
ACG-8	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Ek kontrol	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan bileşenlerin üzerinde kullanılan üçüncü taraf kodlar statik kod analizi ile gözden geçirilmeli ve herhangi bir arka kapı (backdoor) olmadığı doğrulanmalıdır.
ACG-9	Akıllı Cihaz Güvenliği	Tedarik Zinciri Güvenliği	Ek kontrol	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan bileşenler merkezi bir noktadan güvenli bir şekilde güncellenme yeteneğine sahip olmalıdır. [Secure-FOTA (Firmware Over the Air Update) vb.]
ACG-10	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 3	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç mimarisinde yer alan sayaçlar log toplama mekanizmalarını desteklemelidir. Başarılı, başarısız kullanıcı giriş denemeleri, debug fonksiyonlarına erişim denemeleri gibi aktiviteler kayıt altına alınmalıdır. Bunlara ek olarak akıllı cihazlar fiziksel saldırılara karşı da log üretebilmelidir. <i>Bunun sağlanamadığı durumlarda sayaçlara fiziksel ve mantıksal erişimler kısıtlanmalıdır.</i>
ACG-11	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Ek kontrol	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan bileşenlerden alınan log kayıtları en az olay tipi, zaman damgası, kaynak, sonuç bilgilerini içermelidir.
ACG-12	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 3	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan bileşenler güvenilir bir zaman sunucusu üzerinden senkronize edilmeli veya ilgili altyapı bünyesinde bulunan bileşenlerle aynı zamanda olduğu garanti edilmelidir.
ACG-13	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Ek kontrol	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan bileşenlerden alınan loglar üzerinde kritik/hassas bilgilerin olmadığı doğrulanmalıdır. (kriptografik anahtarlar vb.)

ACG-14	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Ek kontrol	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan bileşenlerden alınan loglar, ilgili bileşenler üzerinde ve toplama noktalarında uygun güvenlik kontrolleri ile korunmalıdır. Logların bileşenler üzerinden merkezi noktaya aktarımında güvenli iletişim teknolojileri kullanılmalıdır. (Anlık ya da cihaz üzerinden)
ACG-15	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Log/Kayıt Yönetimi	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında yer alan bileşenlerden alınan logların saklanmasına ilişkin süreler ilgili yasal düzenlemelere uygun olarak belirlenmelidir.
ACG-16	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Yasal Uyumluluk	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında kullanılan bileşenler üzerinde tutulan, işlenen ve saklanan tüm veriler için ilgili yasal düzenlemelere uygun hareket edilmelidir.
ACG-17	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında kullanılan bileşenler üzerinde çalışan servisler belirlenmeli ve gereksiz olduğu değerlendirilen servisler devre dışı bırakılmalıdır.
ACG-18	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısına ilişkin risk analizi sürecinde tüm mimariye ilişkin saldırı vektörleri belirlenmeli ve uygun tehdit modelleme çalışmaları gerçekleştirilmelidir.
ACG-19	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında kullanılan tüm iletişim kanalları ve protokoller belirlenmeli ve dokümanite edilmelidir. (WAN, LAN vb.)
ACG-20	Akıllı Cihaz Güvenliği	Akıllı Sayaç Mimarisi	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç mimarisi uçtan uca belirlenmeli ve dokümanite edilmelidir. Bu dokümantasyon kapsamında tüm bileşenler bir topoloji üzerinden gösterilmelidir.
ACG-21	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında kullanılan tüm cihazlar belirlenerek, bunların üzerindeki erişim arayüzleri (USB, PS2 vb.) uygun seviyede güvenlik kontrolleri ile korunmalıdır. Kullanılmayan veya gereksiz olduğu değerlendirilen arayüzler devre dışı bırakılmalıdır. <i>Bunun sağlanamadığı durumlarda ilgili bileşenlere fiziksel erişimler kısıtlanmalıdır.</i>
ACG-22	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında kullanılan cihazlar üzerindeki debug portları ve CLI (Command Line Interface) erişimleri belirlenerek uygun seviyede güvenlik kontrolleri ile korunmalıdır. <i>Bunun sağlanamadığı durumlarda ilgili bileşenlere fiziksel erişimler kısıtlanmalıdır.</i>
ACG-23	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Ek kontrol	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısı kapsamındaki kritik veriler HSM, SE, TPM vb. içerisinde saklanmalıdır.

ACG-24	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Ek kontrol	Gömülü kod (firmware) snarfing'e karşı uygun güvenlik kontrolleri tanımlanmalı ve korunmalıdır. Bunu sağlamak adına FLASH ve EEPROM alanlarında şifreleme teknikleri uygulanmalıdır. Temel prensip olarak durağan veri (data at rest) güvenliğini sağlamak adına dosya sistemi veya depolama alanlarında şifreleme teknikleri uygulanmalıdır.
ACG-25	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Fiziksel Güvenlik	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında kullanılan cihazların iletişim protokolleri/arayüzleri güvenli şekilde yapılandırılmalıdır. (UART, I2C, SPI vb.) <i>Bunun sağlanamadığı durumlarda ilgili bileşenlere fiziksel erişimler kısıtlanmalıdır.</i>
ACG-26	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç protokolleri replay saldırılarına karşı dirençli olmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
ACG-27	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Haberleşme Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç protokolleri araya girme saldırılarına karşı dirençli olmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
ACG-28	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısı içerisinde hizmet eden sunucular izole bir ağ üzerinde konumlanmalıdır.
ACG-29	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısı içerisindeki izole ağlara erişimler kısıtlanmalıdır. (Uzak erişim, üçüncü taraf, diğer sunucular vb.)
ACG-30	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısı içerisinde hizmet eden sunucular uygun şekilde sıkılaştırılmalıdır. (Veri tabanı, uygulama sunucusu vb.)
ACG-31	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında bulunan veri toplama noktaları arasındaki iletişimler kısıtlanmalıdır.
ACG-32	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısında kullanılan tüm bileşenlerde, gömülü ve basit parola kullanımı engellenmelidir.
ACG-33	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Altyapı Güvenliği	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç altyapısında ağa giriş (access control, port security vb.) kontrolleri uygulanmalıdır.

ACG-34	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Tehdit ve Zafiyet Yönetimi	Seviye 1	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısındaki tüm bileşenlerin "Tehdit ve Zafiyet Yönetimi" başlığının ilgili maddelerine uygunluğu sağlanmalıdır. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
ACG-35	Akıllı Cihaz Güvenliği	Akıllı Sayaçlarda Tehdit ve Zafiyet Yönetimi	Seviye 2	Santral bünyesinde kullanılan ve sahipliği santral işletmesinde olan akıllı/endüstriyel sayaç yapısındaki tüm bileşenler anlık olarak izlenebilir durumda olmalıdır.
ACG-36	Akıllı Cihaz Güvenliği	El Terminallerinin Güvenliği	Seviye 2	Santral bünyesinde el terminallerinin kullanılması durumunda, el terminallerinin istemci ve sunucuları izole ağlar üzerinde konumlandırılmalıdır. Bu ağlara erişimler güvenlik katmanlarından geçirilmelidir.
ACG-37	Akıllı Cihaz Güvenliği	El Terminallerinin Güvenliği	Seviye 2	Santral bünyesinde el terminallerinin kullanılması durumunda, el terminallerinin çalıştığı kablosuz ağlar için güvenlik sıkılaştırmaları uygulanmalıdır.
ACG-38	Akıllı Cihaz Güvenliği	El Terminallerinin Güvenliği	Seviye 2	Santral bünyesinde el terminallerinin kullanılması durumunda, el terminallerinin istemci ve sunucularında güvenlik sıkılaştırmaları uygulanmalıdır.
ACG-39	Akıllı Cihaz Güvenliği	El Terminallerinin Güvenliği	Seviye 2	Santral bünyesinde el terminallerinin kullanılması durumunda, el terminallerinin kontrol sistemleriyle ilişkili herhangi bir erişim ihtiyacı güvenlik katmanları üzerinden sağlanmalıdır.
ACG-40	Akıllı Cihaz Güvenliği	El Terminallerinin Güvenliği	Seviye 2	Santral bünyesinde el terminallerinin kullanılması durumunda, el terminallerinin bulunduğu ağlara, ağ erişim kontrolleri uygulanmalıdır.
ACG-41	Akıllı Cihaz Güvenliği	İzleme Sistemlerinin Güvenliği	Seviye 2	Santral bünyesinde CEMS/SEÖS, SAİS kullanılması durumunda bu bileşenlere ait istemci ve sunucular izole ağlar üzerinde konumlandırılmalıdır. Bu ağlara erişimler güvenlik katmanlarından geçirilmelidir.
ACG-42	Akıllı Cihaz Güvenliği	İzleme Sistemlerinin Güvenliği	Seviye 2	Santral bünyesinde CEMS/SEÖS, SAİS kullanılması durumunda bu bileşenlerde kablosuz ağ kullanması durumunda kablosuz ağlar için güvenlik sıkılaştırmaları uygulanmalıdır.
ACG-43	Akıllı Cihaz Güvenliği	İzleme Sistemlerinin Güvenliği	Seviye 2	Santral bünyesinde CEMS/SEÖS, SAİS kullanılması durumunda bu bileşenlere ait istemci ve sunucularında güvenlik sıkılaştırmaları uygulanmalıdır.
ACG-44	Akıllı Cihaz Güvenliği	İzleme Sistemlerinin Güvenliği	Seviye 2	Santral bünyesinde CEMS/SEÖS, SAİS kullanılması durumunda bu bileşenlerin kontrol sistemleriyle ilişkili herhangi bir erişim ihtiyacı güvenlik katmanları üzerinden sağlanmalıdır.
ACG-45	Akıllı Cihaz Güvenliği	İzleme Sistemlerinin Güvenliği	Seviye 2	Santral bünyesinde CEMS/SEÖS, SAİS kullanılması durumunda bu bileşenlerin bulunduğu ağlara, fiziksel ya da mantıksal ağ erişim kontrolleri uygulanmalıdır.

Endüstriyel Operasyon Güvenliği

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
EOG-1	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik üretim şalt sahası endüstriyel kontrol sistemlerinde (EKS) kullanılan RTU'lar sadece belirli sunuculardan (Master) komut alacak şekilde yapılandırılmalıdır.
EOG-2	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) lojik işleyen bileşenlere sadece mühendislik iş istasyonu üzerinden lojik güncellemeyi sağlayacak kontroller devreye alınmalıdır.
EOG-3	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) mimarisinde kullanılan lojik işleyen bileşenlere lojik güncellemeleri sırasında ek bir parola doğrulaması zorlanmalıdır.
EOG-4	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan DCS ve SCADA konfigürasyon değişimleri sadece yetkili iş istasyonları üzerinden sağlanmalıdır.
EOG-5	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Güvenli Konfigürasyon	Seviye 3	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan DCS ve SCADA konfigürasyon değişimleri sırasında ek bir parola doğrulaması zorlanmalıdır.
EOG-6	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan DCS ve SCADA konfigürasyon dosyaları ve lojik dosyaları için bütünlük kontrolleri devreye alınmalıdır.
EOG-7	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan DCS ve SCADA konfigürasyon dosyaları ve lojik dosyaları sürüm numaraları ile takip edilebilmelidir.
EOG-8	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Erişim ve Yetkilendirme	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan DCS ve SCADA konfigürasyon dosyaları ve lojik dosyalarının saklandığı alanlara sadece yetkili kişi ve grupların eriştiği garanti altına alınmalıdır.
EOG-9	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan DCS ve SCADA konfigürasyon dosyaları ve lojik dosyaları kişisel bulut tabanlı sistemlerde ve dosya paylaşım alanlarında saklanamaz. Bu verilerin kurumsal bulut tabanlı sistemler ve dosya paylaşım alanlarında kullanılmasının zorunlu olduğu durumlarda; T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanarak yayımlanan Bilgi ve İletişim Güvenliği Rehberinde "4.3 Bulut Bilişim Güvenliği" tedbirleri sağlanarak saklanmalıdır.

EOG-10	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyonlarda Veri Güvenliği	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) kullanılan ve üzerinde konfigürasyon veya lojik bilgisi bulunan ekipmanlar kurum dışına çıkarılacaksa (bakım, hibe vb.) söz konusu konfigürasyon ve lojik bilgileri ilgili bileşen üzerinden silinmelidir.
EOG-11	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) yerel HMI (local HMI) kullanılması durumunda kontrol işlemleri sırasında ikinci bir onay mekanizması devreye alınmalıdır. Bunun sağlanamadığı durumlarda ilgili bileşenlere fiziksel erişimler kısıtlanmalıdır.
EOG-12	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) ana kontrol sistemi (DCS) ile yerel kontrol sistemi (lokal HMI) değişiklikler sonrası senkronize olabilmelidir.
EOG-13	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) lojik işleyen bileşenler üzerinde kritik eşik değerleri (trip değerleri) HMI üzerinden sadece izlenebilmeli, HMI üzerinden değiştirilmesine imkan verilmemelidir.
EOG-14	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Seviye 3	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonlara ilişkin tüm operasyonel değer zorlama/baskılama (force etmek, forslama) işlemlerine ait loglar(kayıtlar) sistemler üzerinde otomatik olarak oluşturulmalı ve saklanmalıdır.
EOG-15	Endüstriyel Operasyon Güvenliği	Endüstriyel Operasyon Güvenliği	Ek Kontrol	Elektrik üretim endüstriyel kontrol sistemlerinde (EKS) endüstriyel operasyonlara ilişkin kritik değer aralıklarının dışında gelen değer zorlama/baskılama (force etmek, forslama) işlemleri lojik işleyen bileşenler üzerinde durdurulmalıdır.
EOG-16	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 3	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ek olarak kullanılan safety/emniyet PLC'leri veya Emniyet Kontrol Sistemleri (Safety Instrument System) ağ seviyesinde izole edilmelidir. (Bu izolasyon hard-wired haberleşmeler yapılarak sağlanabilir.) Ağ seviyesinde izole edilemeyen entegre emniyet PLC'leri, endüstriyel prosesi yöneten dağıtık kontrol sistemleri (DCS) ile sadece tek yönlü ve salt okunabilir (read-only) haberleşmelidir.
EOG-17	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 2	Elektrik üretim endüstriyel kontrol sistemlerine (EKS) ek olarak kullanılan safety/emniyet PLC'leri lojik seviyesinde ana kontrol sistemi bileşenlerinden izole edilmelidir. Bunu sağlamak için ana kontrol sistemi ve emniyet/safety işlemlerini yürüten bileşenler cihaz seviyesinde ayrıştırılmalıdır.

EOG-18	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Ek kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda dağıtık kontrol sistemi (DCS) ve safety/emniyet PLC'leri arasındaki veri iletişimi hardwired kanallar üzerinden gerçekleştirilmelidir.
EOG-19	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda kullanılan ekipman ve protokoller, ilgili sistemin risk analizi sonucuna uygun olarak SIL güvenlik mekanizmalarına sahip olmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
EOG-20	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 3	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet PLC'lerinin veya Emniyet Kontrol Sistemleri (Safety Instrument System) kullanıldığı altyapılarda, safety/emniyet PLC bileşenleri bu işe özelleşmiş uygun ekipmanlardan seçilmeli ve yedekli yapıda kurgulanmalıdır.
EOG-21	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Ek Kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda, emniyet kontrol sistemi (SIS) bileşenleri kapsamında aktif izin kullanılıyorsa, bu aktif izin hem dağıtık kontrol sistemi domain yapılarından hem de kurumsal bilgi sistemleri domain yapılarından mantıksal ve fiziksel olarak ayrıştırılmalıdır.
EOG-22	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Ek Kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda, emniyet kontrol sistemi (SIS) bileşenleri kapsamında aktif izin kullanılıyorsa, Yetkinlik Modeli Teknik Kontrol Maddeleri "02-İstemci Sunucu Güvenliği" altında yer alan aktif izin/OT domain güvenliği maddeleri uygulanmalıdır.
EOG-23	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Ek Kontrol	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda, bu altyapılara ait tüm bileşenlere Yetkinlik Modeli Teknik Kontrol Maddeleri tümüyle uygulanmalıdır.
EOG-24	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda, emniyet kontrol sistemi (SIS) bileşenlerine ağ üzerinden uzak erişimler kapatılmalıdır.

EOG-25	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda, emniyet kontrol sistemi (SIS) bileşenlerine kablosuz ya da endüstriyel kablosuz ağlar üzerinden entegrasyon sağlanmamalıdır.
EOG-26	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda, emniyet kontrol sistemi (SIS) bünyesinde yer alan lojik işleyen bileşenler "programlama modu"nda bırakılmamalıdır. Tüm lojik işleyen bileşenler "run mode" olacak şekilde çalıştırılmalıdır.
EOG-27	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde Safety/Emniyet sistemlerinin kullanıldığı altyapılarda, emniyet kontrol sistemi (SIS) bünyesinde gerçekleştirilecek değişiklikler(Mimari, güvenlik cihazı kuralı, yazılım, enstrüman, işletim sistemi vb.) için talepler ilgili BT veya OT birim/ekiplerince de onaylanmalıdır.
EOG-28	Endüstriyel Operasyon Güvenliği	Emniyet/Safety Sistemleri	Seviye 2	Elektrik üretim endüstriyel kontrol sistemleri (EKS) bünyesinde emniyet mekanizmalarını sağlamak için emniyet kontrol sistemlerine (SIS) ek olarak mekanik güvenlik önlemleri de alınmalıdır.

İnsan Kaynakları Güvenliği

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
İKG-1	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak tüm personel yasal mevzuata uyumlu şekilde, gerekli güvenlik kontrollerinden geçirilmelidir. (Adli sicil, güvenlik soruşturması, referans ve belge kontrolü vb.)
İKG-2	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak personelin, işe uygunluk ve sağlık raporları bulunmalıdır.
İKG-3	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	EKS altyapılarında çalışacak personelle sözleşme imzalanmalıdır. (Bu sözleşmeler gizlilik sözleşmesi şeklinde olabileceği gibi ana sözleşmelerin gizlilik ve siber güvenlik maddelerini içermesi şeklinde de olabilir.)
İKG-4	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	Personelle yapılacak sözleşmelerde siber güvenlik ve gizlilik maddeleri en az aşağıdakileri içermelidir: - Gizli bilginin korunması, - Kurumsal hassas ve kritik bilgilerin korunması, - Kurumun uyguladığı veya uygulayacağı tüm siber güvenlik kontrollerine uyum, - Kuruluşa ait; lojik, konfigürasyon bilgileri, yedek dosyalar ve tasarımların kişisel disk, bilgisayar ya da bulut ortamlarında saklanmayacağına dair beyan, - Yasal, sözleşme kaynaklı veya müşteri gereksinimlerinden doğan siber güvenlik politika, prosedür ve uygulamalarına uyumlu çalışma.
İKG-5	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	İşe alım ilanları, ilgili tesisin siber güvenlik açısından bağlayıcı olan teknolojileri ile ilgili bilgi içermemesini sağlayacak politika, prosedür ve süreçler çerçevesinde tasarlanmalıdır.
İKG-6	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Personel, çalışma süresince tüm siber güvenlik politika, prosedür ve uygulamalarına uyumlu hareket etmelidir.
İKG-7	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Tüm EKS personeli periyodik siber güvenlik farkındalık programına dahil edilmelidir.
İKG-8	İnsan Kaynakları Güvenliği	İstihdam Sırasında	Seviye 1	Siber güvenlik operasyonlarını yürütecek personelin EKS bileşenleri ile ilgili eğitim almaları sağlanmalıdır.
İKG-9	İnsan Kaynakları Güvenliği	İstihdam Öncesi	Seviye 1	Tüm EKS personeli için siber güvenlik ihlallerine ilişkin disiplin süreçleri tanımlanmalıdır.
İKG-10	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	Sözleşme ve uygulamalar, istihdam sonrası koşulları içermelidir.
İKG-11	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdamın sonlandırılması ile birlikte tüm EKS varlıklarına olan mantıksal ve fiziksel erişimler sonlandırılmalıdır.

İKG-12	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdam sonlanması ile birlikte tüm gerekli taraflar bilgilendirilmelidir.
İKG-13	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İstihdam sonlanması sürecinde operasyonel süreklilik için önem arz eden tüm varlıklar (proses, lojik vb.) güvenli bir şekilde devredilmelidir.
İKG-14	İnsan Kaynakları Güvenliği	İstihdam Sonrası	Seviye 1	İlgili istihdam sonlandırma süreci, olaylı ayrılma durumlarını da içermelidir.
İKG-15	İnsan Kaynakları Güvenliği	Üçüncü Taraf Güvenliği	Seviye 1	EKS altyapılarında üçüncü taraflarca sağlanan taşeron personellerin hem birinci derece bağlı oldukları hem de hizmet sundukları kuruluşlar için "İnsan Kaynakları Güvenliği" başlığı altındaki süreçler işletilmelidir. Alt yükleniciler, farklı bir alt yüklenici kullandığında sorumluluk devredemeyeceği gibi bu madde kapsamında doğan yükümlülüklerinin yerine getirilmesi konusunda kendi alt yüklenicilerinden sözleşmesel taahhüt alacaktır.
İKG-16	İnsan Kaynakları Güvenliği	Üçüncü Taraf Güvenliği	Seviye 1	EKS altyapılarında üçüncü taraflara veya üreticiye bağlı olarak çalışan personel, kuruluşun belirlediği gizlilik ve siber güvenlik gereksinimlerinden muaf tutulamaz. Gerekli koşullarda ilgili personelle de ek bir gizlilik sözleşmesi veya siber güvenlik maddelerini içeren sözleşme yapılmalıdır.

Fiziksel Güvenlik

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
FZG-1	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke girişinde giriş çıkış kaydı tutulmalıdır.
FZG-2	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke girişinde yetkisiz erişime karşı önlemler alınmalıdır.
FZG-3	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke giriş prosedürleri tanımlanmalıdır. Yerleşke giriş prosedürleri, ziyaretçi, geçici-kalıcı çalışan, acil giriş durumlarını içermelidir.
FZG-4	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke girişlerinde uygun güvenlik ve emniyet eğitimleri verilmelidir.
FZG-5	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde zaman senkronizasyonu sağlanmalıdır.
FZG-6	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde merkezi kayıt yönetim sistemi entegrasyonu sağlanmalıdır.
FZG-7	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke giriş çıkışlarını izleyen elektronik sistemlerde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.
FZG-8	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke çevresini izlemek için kameralar kurulmalıdır. Bu sistemler sürekli olarak izlenmelidir.
FZG-9	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Yerleşke çevresi kamera kayıtları ilgili yasal süre kadar saklanmalıdır.
FZG-10	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Kamera sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-11	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenleri izole ağlarda konumlanmalıdır.
FZG-12	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenlerine erişim kullanıcı adı ve parola ile sağlanmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-13	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Çevresel güvenlik bileşenleri yetkisiz fiziksel erişime karşı korunmalıdır.
FZG-14	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Ek kontrol	Merkezi kontrol sistemi bileşenlerinin bulunduğu alanlara fiziki erişimin tamamıyla kontrol altına alınabileceği herhangi bir noktada X-RAY cihazı konumlandırılmalıdır.
FZG-15	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Seviye 1	Araçlar gerekli kontrollerden geçirilerek yerleşkeye alınmalıdır.
FZG-16	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Ek kontrol	Elektrik üretim yerleşkelerinde insansız hava araçlarına (drone) karşı önlemler alınmalıdır.
FZG-17	Fiziksel Güvenlik	Elektrik Üretim Yerleşke Güvenliği	Ek kontrol	Elektrik üretim yerleşkelerinde kullanılan anti-drone sistemlerinin mevcut elektrik üretim bileşenlerinin çalışmasını olumsuz yönde etkilemeyeceği garanti altına alınmalıdır.
FZG-18	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları giriş ve çıkışlarında kayıt tutulmalıdır.
FZG-19	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları giriş ve çıkışlarında elektronik sistem kullanılması durumunda bu sistemler için zaman senkronizasyonu sağlanmalıdır.
FZG-20	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları giriş ve çıkışlarında elektronik sistemler kullanılması durumunda merkezi kayıt yönetim sistemine entegre edilmelidir.
FZG-21	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları giriş ve çıkışlarında elektronik sistemler kullanılması durumunda yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.

FZG-22	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları giriş ve çıkışlarında elektronik sistemler kullanılması durumunda bu sistemler izole ağlarda konumlandırılmalıdır.
FZG-23	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları çevresel güvenlik bileşenlerine erişim kullanıcı adı ve parola ile sağlanmalıdır.
FZG-24	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları giriş ve çıkışlarında elektronik sistem kullanılması durumunda bu sistemlere güçlü parola kullanılmalıdır.
FZG-25	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarında kurum harici çalışanlara kurum personeli eşlik etmelidir.
FZG-26	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	Kontrol odalarının giriş ve çıkışlarını izlemek için kameralar kurulmalıdır. Bu sistemler sürekli olarak izlenmelidir.
FZG-27	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	DCS odalarının giriş ve çıkışlarını izlemek için kameralar kurulmalıdır. Bu sistemler sürekli olarak izlenmelidir.
FZG-28	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	Kontrol ve DCS odaları kamera kayıtları ilgili yasal süre kadar saklanmalıdır.
FZG-29	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	Kontrol ve DCS odaları kamera sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-30	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	Kontrol ve DCS odaları kamera sistemleri IP tabanlı ise ayrı izole bir ağ üzerinde konumlandırılmalıdır.
FZG-31	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	Kontrol ve DCS odaları kamera bileşenleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-32	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları çevresel güvenlik bileşenleri (Kamera, kartlı geçiş, yangın algılama vb.) yetkisiz fiziksel erişime karşı korunmalıdır.
FZG-33	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	Kontrol ve DCS odalarında bulunan kameralar proseslerin izlendiği HMI'ları görmeyecek şekilde konumlandırılmalıdır.
FZG-34	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	Kontrol odalarının kapıları otomatik olarak kapanmalıdır.
FZG-35	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	DCS odalarının kapıları otomatik olarak kapanmalıdır.
FZG-36	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol odalarından acil çıkış mümkün olmalıdır.
FZG-37	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Ek kontrol	DCS odalarından acil çıkış mümkün olmalıdır.
FZG-38	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarında yer alan çevresel izleme sensörleri yetkisiz fiziksel erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-39	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 2	Kontrol ve DCS odalarının kapıları açık kaldığında alarm üretmelidir.
FZG-40	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarına çevresel izleme sensörleri konumlandırılmalıdır. (Yangın, su, nem, sıcaklık vb.)
FZG-41	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarında kullanılan çevresel izleme sistemleri alarm üretebilmelidir.
FZG-42	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları çevresel izleme sensörleri merkezi olarak izlenmelidir.

FZG-43	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları yangın koruma/söndürme sistemleri bulundurulmalıdır.
FZG-44	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları yangın koruma/söndürme sistemlerinin periyodik bakımları yapılmalıdır.
FZG-45	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları yangın koruma/söndürme sistemleri elektronik ortamlar için uygun olmalıdır.
FZG-46	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları uygun iklimlendirme altyapısına sahip olmalıdır.
FZG-47	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları giriş kontrolleri, enerjisiz kaldığında da aynı güvenlik seviyesini korumalıdır.
FZG-48	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarında yedek enerji besleme kaynakları bulundurulmalıdır.
FZG-49	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarındaki tüm güvenlik bileşenleri yedek bir enerji ya da kesintisiz bir enerji kaynağı üzerinden beslenmelidir.
FZG-50	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 2	Endüstriyel operasyonlara hizmet eden istemci ve sunuculara fiziksel erişimler kısıtlanmalıdır.
FZG-51	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarında bulunan ve endüstriyel operasyona hizmet eden bileşenlerin bulunduğu kabinler fiziksel erişime imkan vermeyecek şekilde konumlandırılmalıdır.
FZG-52	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları bünyesinde deprem koruma önlemleri alınmalıdır.
FZG-53	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları bünyesinde su baskını koruma önlemleri alınmalıdır.
FZG-54	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarında kablolama güvenliği ilkeleri uygulanmalıdır.
FZG-55	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odalarında kablolar etiketlenmelidir.
FZG-56	Fiziksel Güvenlik	Kontrol ve DCS Odaları	Seviye 1	Kontrol ve DCS odaları bünyesinde enerji besleme bileşenlerinin periyodik bakımları gerçekleştirilmelidir.
FZG-57	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi hizmetlerinin üçüncü taraflardan temin edilmesi durumunda; alınması gerekli tedbirler sözleşmeler ile hüküm altına alınmalıdır. Paylaşımlı veri merkezlerinde tüm tarafların güvenliği ve gizliliği hizmet sağlayıcı tarafından güvence altına alınmalıdır.
FZG-58	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi giriş-çıkış kayıtları tutulmalıdır.
FZG-59	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi elektronik geçiş kontrol sistemlerinde zaman senkronizasyonu sağlanmalıdır.
FZG-60	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi elektronik geçiş kontrol sistemlerinde merkezi log/kayıt yönetim entegrasyonu sağlanmalıdır.
FZG-61	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi elektronik geçiş kontrol sistemlerinde yedekleme politikaları oluşturulmalı, yedekler alınmalı ve yedekler test edilmelidir.
FZG-62	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi elektronik geçiş kontrol sistemleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-63	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi ziyaretlerinde yetkili personel ziyaretçilere eşlik etmelidir. Ziyaretçi ve refakatçi kayıtları en az bir yıl süre ile saklanmalıdır.
FZG-64	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezini izlemek için kamera sistemi kurulmalıdır.

FZG-65	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesindeki kameralara ilişkin kayıtlar belirlenen yasal süre kadar saklanmalıdır.
FZG-66	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesindeki kameralarda zaman senkronizasyonu sağlanmalıdır.
FZG-67	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesindeki kamera bileşenlerinin IP tabanlı olması durumunda bu bileşenler mantıksal izole bir ağ üzerinde konumlandırılmalıdır.
FZG-68	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesindeki kamera bileşenleri kullanıcı adı ve parola ile korunmalıdır. Erişim için güçlü parolalar kullanılmalıdır.
FZG-69	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesindeki kameralar fiziksel erişime karşı koruma altına alınmalıdır.
FZG-70	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesindeki kameralar kör nokta olmaksızın konumlandırılmalıdır.
FZG-71	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi giriş çıkış kapıları otomatik olarak kapanmalıdır.
FZG-72	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi giriş çıkış kapıları acil çıkış prosedürlerine uygun olmalıdır.
FZG-73	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi giriş çıkış noktalarında olan sensörler yetkisiz erişime olanak vermeyecek şekilde konumlandırılmalıdır.
FZG-74	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 2	Sunucu odası veya veri merkezi kapıları açık kaldığında alarm üretebilmelidir.
FZG-75	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesinde çevresel izleme sensörleri konumlandırılmalıdır.
FZG-76	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi çevresel izleme sensörleri alarm üretme kabiliyetine sahip olmalıdır.
FZG-77	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi çevresel izleme sensörleri merkezi olarak izlenebilmelidir.
FZG-78	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi giriş çıkış kontrolleri, elektrik kesintilerinde aynı koruma seviyesine sahip olmalıdır.
FZG-79	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi çevresel izleme bileşenleri yedek enerji kaynaklarıyla ya da kesintisiz enerji kaynakları üzerinden beslenmelidir.
FZG-80	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesinde deprem koruma önlemleri alınmalıdır.
FZG-81	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesinde su baskını koruma önlemleri alınmalıdır.
FZG-82	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi yangın koruma/söndürme sistemleri bulundurulmalıdır.
FZG-83	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi yangın koruma/söndürme sistemlerinin periyodik bakımları yapılmalıdır.
FZG-84	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi yangın koruma/söndürme sistemleri elektronik ortamlar için uygun olmalıdır.
FZG-85	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi uygun iklimlendirme altyapısına sahip olmalıdır.
FZG-86	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesinde kablolama güvenliği ilkeleri uygulanmalıdır.
FZG-87	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesinde kablolar etiketlenmelidir.

FZG-88	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesinde yedek enerji besleme kaynakları bulundurulmalıdır.
FZG-89	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Seviye 1	Sunucu odası veya veri merkezi bünyesinde enerji besleme bileşenlerinin periyodik bakımları gerçekleştirilmelidir.
FZG-90	Fiziksel Güvenlik	Sunucu Odası veya Veri Merkezi	Ek Kontrol	Veri merkezleri en az TIER-III sertifikasına sahip olmalı ya da bu sertifikayı sağlayan ülke içi veri merkezlerinden hizmet alınmalıdır.

Tedarikçi Yönetimi				
No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
TDY-1	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluşun tedarikçiye olan bağımlılıklarını belirlemek için bağımlılık kriterleri tanımlanmalıdır.
TDY-2	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim endüstriyel kontrol sistemlerinin (EKS) devamlılığının sağlanması için önem arz eden tüm EKS (EKS ile etkileşimi olan KBS varlıklarını da içerecek şekilde) tedarikçileri ve bu tedarikçilerin bağımlılıkları belirlenmelidir.
TDY-3	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tüm kritik veya tekil kaynak bağımlılıklarını tanımlamalıdır.
TDY-4	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tedarikçileri bağımlılıklarına göre önceliklendirmelidir.
TDY-5	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler ve diğer bağımlılıklardan kaynaklanan önemli siber güvenlik riskleri tanımlanmalı ve adreslenmelidir.
TDY-6	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluş, tedarikçi bağımlılıklarından kaynaklanan risk yönetimi aktivitelerini, mevcut risk yönetim süreçlerine dahil etmelidir.
TDY-7	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçiler ve diğer üçüncü taraflar ile yapılan sözleşmelerde siber güvenlik gereksinimleri dikkate alınmalıdır. <i>(Bu kontrol; mevcut sözleşmelerde bulunmuyorsa, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-8	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü taraflarla (üretici, mühendislik firmaları, altyükleniciler) yapılan sözleşmeler ve anlaşmalar aşağıdakileri içermelidir: - Üçüncü tarafların sunduğu ürün ve hizmetlerde ortaya çıkan zafiyetlere ilişkin sorumluluklar, - Üçüncü tarafların kendisine ya da sunduğu ürünlere yönelik saldırı/tehdit bilgilerini kuruluşlarla paylaşma ilkeleri <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>

TDY-9	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Yazılım geliştirme yapan ya da yazılım hizmeti sunan tedarikçiler kuruluşlara sunduğu ürün ve hizmetler için güvenli yazılım geliştirme süreçleri de dahil olacak şekilde siber güvenlik kontrollerine sahip olmalıdır. Sunulan ürün ve hizmetler bu kontrollere uygun olarak yürütülmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-10	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Tedarikçiler ile yapılan sözleşmeler, tedarikçinin sağladığı hizmetlerin sahip olduğu veya gelecekte oluşabilecek güvenlik açıklarını bildirme sürecini içermelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-11	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçi tarafından sağlanan tüm yazılım ve yamaların bütünlüğü ve orijinallliği kontrol edilerek bu yazılım ve yamaların değiştirilmediği garanti altına alınmalıdır.
TDY-12	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçilerin sisteme uzaktan erişim için talepleri kapsamında dokümanite edilmiş uzak erişim bağlantı süreçleri ve kontrol yöntemleri tanımlanmalıdır. Tedarikçi erişimleri "Kimlik ve Erişim Yönetimi" başlığına uygun olarak yürütülmelidir. Bu madde ile atıfta bulunulan başlıklarda yer alan maddelerin uygulamaları, ilgili başlıklar altında maddelere tanımlanan sürelerde tamamlanmalıdır.
TDY-13	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçi ile yapılan sözleşmelerde, elektrik üretim endüstriyel kontrol sistemlerinin (EKS) sürekliliğini tehdit eden arıza ve problemlere müdahale süreçleri belirlenmeli ve oluşabilecek riskler, risk yönetim sürecine dahil edilmelidir.
TDY-14	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Tedarikçilerin ve diğer harici kuruluşların değerlendirilmesi ve seçimi süreçlerinde, tedarikçilerin siber güvenlik gereksinimlerini karşılama yetenekleri değerlendirilmelidir.
TDY-15	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Tedarikçilerle yapılan sözleşmeler ya da yapılacak işi tanımlayan teknik şartnameler, bir siber güvenlik olayı veya ihlaline ilişkin bildirimleri de içermelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>

TDY-16	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluşun bilgi varlıklarına geçici ya da kalıcı olarak erişebilen (uzak erişimler de dahil olmak üzere), bunu işletebilen, depolayabilen, iletebilen veya kuruluşun bilgi varlıkları için KBS altyapı bileşenlerini temin eden tedarikçilerin her biri ile sözleşme yapılmalı ve sözleşmeler bilgi güvenliği gereksinimlerini içermelidir.
TDY-17	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Üçüncü taraflardan doğan risklere ilişkin azaltıcı/yok edici kontroller uygulanmalıdır.
TDY-18	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 1	Kuruluş tarafından üçüncü taraflara yönelik uygulanacak siber güvenlik kontrolleri, üçüncü tarafın kritikliğine ve risk seviyesine uyarlanabilir olmalıdır.
TDY-19	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü taraf siber güvenlik süreç yönetiminde ve seçiminde destek sonu (end of support), ömür sonu (end of life) durumları göz önünde bulundurulmalı, sözleşmelere dahil edilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
TDY-20	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü tarafların lisanslı olmayan ürün sağlamasının önüne geçilmelidir. Bu konuyla ilgili oluşabilecek güvenlik ihlalleri sözleşme ya da teknik şartnamelerde ele alınmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır)</i>
TDY-21	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Siber güvenlik gereksinimlerinin karşılanmasına ilişkin kabul testleri (SAT ve FAT) tanımlanmalı ve gerçekleştirilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır)</i>
TDY-22	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Tedarikçi Risk Yönetimi	Seviye 2	Üçüncü tarafların siber güvenlik kapasite yeterliliği periyodik olarak gözden geçirilmeli, tanımlı metriklerle ölçülmelidir. İşletmeler, belirli puanın altında kalan tedarikçilerle olan çalışmalarını gözden geçirmelidir.
TDY-23	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Kuruluş, tedarikçilerden doğan değişiklikleri yönetmelidir. Bu değişikliklerin siber güvenlik risk durumuna olan etkileri risk yönetim süreci kapsamında ele alınmalıdır.
TDY-24	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflara yönelik uygulanacak politika ve prosedürler periyodik olarak veya ihtiyaçlara uygun şekilde güncellenmelidir.

TDY-25	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflarla olan ilişkileri yöneten ve hizmetleri sağlayan personelde gerekli siber güvenlik yetkinlikleri aranmalıdır. Yetkinliklere ilişkin şartlar sözleşmelerle ya da teknik şartnamelerle garanti altına alınmalıdır.
TDY-26	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflarla olan ilişkileri yöneten personele ilişkin sorumluluklar, yetki ve hesap verilebilirlik durumu dokümente edilmiş olmalıdır.
TDY-27	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü taraflara ilişkin aktiviteler(itibar durumları, veri sızıntısı, hedefli saldırı, zararlı yazılım, fidye vb. saldırılara karşı durumları vb.) sürekli olarak izlenmeli ve değerlendirilmelidir.
TDY-28	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Üçüncü tarafların hizmet sunduğu kuruluşa ait bilgileri halka açık ağlarda izinsiz yayınlamayacağı ve referans gösteremeyeceği hususu şartnameler ya da sözleşmelerle garanti altına alınmalıdır.
TDY-29	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim tesisi kapsamında endüstriyel operasyonların yönetiminde sözleşmelerle tariflenen üretici ya alt yüklenici tabanlı uzaktan yönetim ve izleme işlemleri yapılıyorsa, üretici veya alt yüklenicinin yetkinlik modelinde yer alan idari ve teknik kontrollere uyumluluğu şartnameler ya da sözleşmelerle garanti altına alınmalıdır.
TDY-30	Tedarik Zinciri ve Dış Bağlılıklar Yönetimi	Politika, Prosedür, Süreç	Seviye 1	Elektrik üretim tesisi kapsamında endüstriyel operasyonların yönetiminde sözleşmelerle tariflenen üretici ya alt yüklenici tabanlı yerinde yönetim ve izleme işlemleri yapılıyorsa, üretici veya alt yüklenicinin yetkinlik modelinde yer alan idari ve teknik kontrollere uyumluluğu şartnameler ya da sözleşmelerle garanti altına alınmalıdır.

PLC Güvenliđi

No	Ana Kontrol	Alt Kontrol	Seviye	Kontrol
PLC-1	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	Oluřturulacak DCS Kontrolc (Controller), ana veya destekleyici proses PLC yazılımında kodlar modlerize edilerek farklı fonksiyon blokları kullanılmalı ve oluřturulan modller ve bu fonksiyon blokları SAT ve FAT sreçlerinde test edilebilmelidir. Endstriyel reticilerin DCS Kontrolc ya da PLC'leri zerinde bulunan lojiklerin ticari sır ihtiva ettiđi durumlarda bu maddeye iliřkin uyumluluđun sađlandığına dair retici veya alt ykleniciden taahht alınmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu dzenleme yrrlđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)
PLC-2	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	DCS Kontrolc (Controller), ana veya destekleyici proses PLC'leri destekliyorsa, PLC alıřma modları takip edilmeli ve RUN modunda deđilse HMI veya grntleme bileřenleri zerinde alarm retilmelidir. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu dzenleme yrrlđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)
PLC-3	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	Lojik iřlemleri mmkn ise DCS Kontrolc (Controller), ana veya destekleyici proses PLC'leri zerinde yapılmalıdır. HMI ve grntleme bileřenleri zerinde operasyonel lojik yazmaktan kaınılmalıdır.
PLC-4	PLC Güvenliđi	PLC Güvenliđi	Ek Kontrol	Oluřturulan yazılımda btnlk kontroln sađlamak iin lojik flag'leri kullanılmalı, matematiksel hatalarda, saya (counter) tařmasında, negatif sayalarda hata flagleri retilmelidir. Endstriyel reticilerin DCS Kontrolc ya da PLC'leri zerinde bulunan lojiklerin ticari sır ihtiva ettiđi durumlarda bu maddeye iliřkin uyumluluđun sađlandığına dair retici veya alt ykleniciden taahht alınmalıdır.
PLC-5	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolc (Controller), ana veya destekleyici proses PLC'lerinde kod btnlđn korumak ve yazılım deđiřtiđinde alarm retmek iin, endstriyel retici desteđi varsa checksum zellikleri kullanılmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu dzenleme yrrlđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)

PLC-6	PLC Güvenliği	PLC Güvenliği	Seviye 3	Zamanlayıcı (timer) ve sayaç (counter) değerleri DCS Kontrolcü (Controller), ana veya destekleyici proses PLC programına yazıldığında ikincil bir kontrol olarak bu değerlerin geçerlilik kontrolü yapılmalıdır. Endüstriyel üreticilerin DCS Kontrolcü ya da PLC'leri üzerinde bulunan lojiklerin ticari sır ihtiva ettiği durumlarda bu maddeye ilişkin uyumluluğun sağlandığına dair üretici veya alt yükleniciden taahhüt alınmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
PLC-7	PLC Güvenliği	PLC Güvenliği	Seviye 3	Her iki sinyalin aynı anda gelemeyeceği durumlar için sinyaller eşleştirilmeli ve ikisinin aynı anda verilmediğinden emin olunmalı ayrıca fiziksel olarak mümkün olmayan giriş çıkış durumları oluştuğunda alarm üretilmelidir. Endüstriyel üreticilerin DCS Kontrolcü ya da PLC'leri üzerinde bulunan lojiklerin ticari sır ihtiva ettiği durumlarda bu maddeye ilişkin uyumluluğun sağlandığına dair üretici veya alt yükleniciden taahhüt alınmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
PLC-8	PLC Güvenliği	PLC Güvenliği	Seviye 3	DCS Kontrolcü (Controller), ana veya destekleyici proses PLC değişkenlerine HMI erişimi HMI'da belirlenen operasyonel değer aralığı ile sınırlandırılmalı ayrıca değer aralığı dışındaki değerler için de bileşen üzerinde çapraz sorgulamalar yapılmalıdır. Endüstriyel üreticilerin DCS Kontrolcü ya da PLC'leri üzerinde bulunan lojiklerin ticari sır ihtiva ettiği durumlarda bu maddeye ilişkin uyumluluğun sağlandığına dair üretici veya alt yükleniciden taahhüt alınmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)
PLC-9	PLC Güvenliği	PLC Güvenliği	Seviye 3	DCS Kontrolcü (Controller), ana veya destekleyici proses PLC yazılımında bir register değerinin başka bir registerda kullanılmadığından emin olunmalı ve bunun için önlemler alınmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüğe girdiği andan itibaren kurulacak olan altyapılarda aranacaktır.)

PLC-10	PLC Güvenliđi	PLC Güvenliđi	Ek Kontrol	DCS Kontrolc (Controller), ana veya destekleyici proses PLC yazılımında tanımlanmış sinyallere harici yazmaları engellemek, verileri doğrulamak ve korumak, arabellek taşmalarını engellemek için daha önceden belirlenmiş kayıt blokları atanmalıdır.
PLC-11	PLC Güvenliđi	PLC Güvenliđi	Ek Kontrol	DCS Kontrolc (Controller), ana veya destekleyici proses PLC yazılımında tanımlanmış farklı proses ekipmanlarının ölçm değeri lerinin doğruluk kontrol için çapraz kontroller yapılmalı ve alarm üretilmelidir. Endstriyel üreticilerin DCS Kontrolc ya da PLC'leri üzerinde bulunan lojiklerin ticari sır ihtiva ettiđi durumlarda bu maddeye ilişkin uyumluluđun sađlandığına dair üretici veya alt yükleniciden taahht alınmalıdır.
PLC-12	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolc (Controller), ana veya destekleyici proses PLC yazılımına pratikte fiziksel olarak mümkün değeri lerin girildiğinden emin olunmalı ve bunun yanı sıra fiziksel olarak olması gereken süreler dışında bir gecikme veya sapmada alarm üretilmelidir. Endstriyel üreticilerin DCS Kontrolc ya da PLC'leri üzerinde bulunan lojiklerin ticari sır ihtiva ettiđi durumlarda bu maddeye ilişkin uyumluluđun sađlandığına dair üretici veya alt yükleniciden taahht alınmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürrlđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)
PLC-13	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolc (Controller), ana veya destekleyici proses PLC'lerde ön tanımlı (default) olarak aktif gelen ve kullanılmayan haberleşme protokolleri, servisler ve portlar devre dışı bırakılmalıdır.
PLC-14	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolc (Controller), ana veya destekleyici proses PLC'lerde ile haberleşecek 3. parti arayzler veya uygulamalar için bađlantı trleri ve paylaşılan veriler kısıtlanmalı yalnızca gerekli veriler üzerinden okuma yazma yetkilerine izin verecek şekilde konfigrasyon yapılmalıdır.
PLC-15	PLC Güvenliđi	PLC Güvenliđi	Seviye 2	DCS Kontrolc (Controller), ana veya destekleyici proses PLC'nin tekrar başlaması durumunda proses için güvenli bir durum tanımlanmalıdır. Endstriyel üreticilerin DCS Kontrolc ya da PLC'leri üzerinde bulunan lojiklerin ticari sır ihtiva ettiđi durumlarda bu maddeye ilişkin uyumluluđun sađlandığına dair üretici veya alt yükleniciden taahht alınmalıdır. (Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürrlđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)

PLC-16	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolcü (Controller), ana veya destekleyici proses PLC çevrim (cycle) zamanı her iki veya üç saniyede bir özetlenerek HMI'da trend olarak gösterilmelidir. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
PLC-17	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolcü (Controller), ana veya destekleyici proses PLC çalışma süresi kayıt altına alınarak HMI tarafında izlenmelidir.
PLC-18	PLC Güvenliđi	PLC Güvenliđi	Ek Kontrol	Arıza ve kapanmalardan kaynaklanan DCS Kontrolcü (Controller), ana veya destekleyici proses PLC duruşları kayıt altına alınmalı ve HMI tarafında izlenmelidir.
PLC-19	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolcü (Controller), ana veya destekleyici proses PLC yazılımının hafıza kullanımı ölçülmeli, kuruluş tarafından belirlenen eşik değeri aşımı alarmlaştırılmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>
PLC-20	PLC Güvenliđi	PLC Güvenliđi	Seviye 3	DCS Kontrolcü (Controller), ana veya destekleyici proses PLC yazılımında proses için kritik alarm ve uyarılar belirlenmeli ve bu uyarılar için false pozitif ve false negatif durumları karşılayacak lojik düzenlemeleri yapılmalıdır. <i>(Bu kontrol, altyapı yenileme projeleri sırasında ya da bu düzenleme yürürlüđe girdiđi andan itibaren kurulacak olan altyapılarda aranacaktır.)</i>