TÜRKİYE BÜYÜK MİLLET MECLİSİ

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ POLİTİKALARI

1. AMAÇ

Bilgi Güvenliği Yönetim Sistemi (BGYS) politikalarının amacı; Türkiye Büyük Millet Meclisi (TBMM) bilişim sistemlerinin, bilgi ve varlıklarının; gizlilik, bütünlük ve erişilebilirlik bakımından uyulması gereken iş kurallarını belirlemek ve bu kurallar kapsamında iş sürekliliğini sağlamaktır.

BGYS politikaları ile Kurum, herhangi bir kimse üzerinde kısıtlayıcı kurallar oluşturmayı değil aksine kurumsallaşma, şeffaflık, bilgi güvenliği ve bütünlüğüne yönelik kültürü yerleştirmeyi hedeflemektedir. TBMM'de kullanılan bilgi teknolojileri Kurumun sahip olduğu değerlerdir. Güçlü bir bilgi güvenliği Kurum çalışanlarının dâhil olduğu takım çalışmasıyla gerçekleştirilir. Bilgi güvenliğinin sağlanabilmesi için Kurum çalışanlarının bilgi güvenliği politikalarını iyi bilmesi ve uygulanmasının sorumluluğunu taşıması gerekmektedir.

2. KAPSAM

Kurum bilişim kaynaklarını kullanan kullanıcıları ve Başkanlık tarafından verilen hizmetleri kapsamaktadır.

3. YAPTIRIM

Bu politikalara uyulmaması halinde sorumlu kullanıcılar hakkında ilgili kanunların disiplin ve cezaya ilişkin hükümleri uygulanır. Ayrıca tedarikçi, ziyaretçi ve geçici görevli olarak gelenler için ise genel hükümler uygulanarak yasal süreç başlatılacaktır.

4. SORUMLULAR

BGYS politikaları Türkiye Büyük Millet Meclis Başkanlığı tarafından onaylanır ve Genel Sekreterlik tarafından duyurulması sağlanır. Bu politikaların gözden geçirilmesi ve güncellenmesinden Başkanlık sorumlu olup kullanıcılar, tedarikçi, ziyaretçiler ve geçici görevli olarak gelenler uymakla yükümlüdür.

5. KISALTMA ve TANIMLAR

Kurum: Türkiye Büyük Millet Meclisi Başkanlığını,

Başkanlık: Bilgi İşlem Başkanlığını,

Kurum Ağı: Türkiye Büyük Millet Meclisi Başkanlığının sunduğu İnternet/İntranet hizmetini,

Tedarikçi: TBMM'ye ürün ya da hizmet sağlayan gerçek/tüzel kişilikleri,

Ziyaretçi: TBMM'ye ziyaret, görev veya iş nedeniyle gelen kişileri,

Paydaş: TBMM'nin hizmet verdiği veya aldığı tedarikçi, ziyaretçi ve kamu kurum ve kuruluşlarını,

Kullanıcı: TBMM Bilişim kaynağını kullanan herkesi,

İdari Teşkilat: TBMM idari teşkilatını,

BGYS: Bilgi Güvenliği Yönetim Sistemini,

SOME: Bilgi İşlem Başkanlığı bünyesinde oluşturulan Siber Olaylara Müdahale Ekibini,

Bilişim Kaynakları: Mülkiyet hakları TBMM'ye ait olan ve/veya lisanslanan ya da kullanım hakkına sahip olunan veriler, bilgi ve belgeler dâhil olmak üzere her türlü bilgisayar, yazıcı, tarayıcı, mobil cihazlar, bilgisayar ağı, donanım, yazılım ve hizmetleri (Kurumsal hizmetler, e-posta, internet vb.),

Uzak bağlantı; Kurum bilişim kaynaklarına, TBMM hizmet binaları içinden veya dışından görevi gereği olmak koşulu ile bilgisayar veya mobil cihazlar üzerinden erişim sağlanması,

6. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMA POLİTİKALARI

6.1. AĞ VE İNTERNET ERİŞİM POLİTİKASI

6.1.1. Amaç

Kurum ağından güvenli internet/intranet erişiminin sağlanması için gereken standart ve kuralların belirlenmesi ve uygulanması amaçlanmaktadır.

İnternet/intranet erişiminin uygun olmayan kullanımı; Kurumun yasal yükümlülükleri, kapasite kullanımı ve Kurum imajı açısından istenmeyen sonuçlara neden olabilir. Bu tür olumsuzlukların gerçekleşmemesi için internet/intranet kullanım kurallarını düzenlemek gerekmektedir.

6.1.2. Kapsam

Bu politika Kurum bilişim kaynaklarını kullanan kullanıcıları kapsamaktadır.

6.1.3. Politika

6.1.3.1. ***5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*** gereğince Kurum internet erişim kayıtlarının belirlenen süre boyunca tutulması gerekmektedir.

6.1.3.2. Kurum ağı üzerinden film, dizi, müzik, program vb. içerikleri indirmek ve yasalara aykırı internet sitelerini ziyaret etmek yasaktır.

6.1.3.3. Kurum ağında BGYS politikalarına aykırı hiçbir teknoloji, program, metot vb. kullanılamaz.

6.1.3.4. Başkalarının fikri haklarını ihlal edici mahiyette materyalin (yazı, makale, kitap, film, müzik eserleri vb.) dağıtımı yasaktır.

6.1.3.5. Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır. Kurum bu tür ihlalleri tespit etmesi halinde ilgililer hakkında disiplin ve soruşturma süreçlerini başlatır.

6.1.3.6. Kurum ağı kullanılarak uygunsuz, müstehcen, rahatsız edici materyaller ve Kurumsal bilgileri yayınlamak, paylaşmak yasaktır.

6.1.3.7. Kurum ağı kullanılarak Türkiye Cumhuriyeti Devletine, vatandaşlarına, Kurum ve kuruluşlarına yönelik iftira ve karalama mahiyetinde mesajlar yayınlamak, paylaşmak yasaktır.

6.1.3.8. Kullanıcıların, Kurum ağını kullanarak görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek yayınlar yapan televizyon, radyo, film, canlı kamera yayınları, sosyal medya, oyun vb. içerikli yayınlara erişimi yasaktır.

6.1.3.9. Kullanıcıların, Kurum ağı üzerinden yaptığı kişisel işlemlerde (banka, alışveriş, e-posta vb.) oluşacak olumsuzluklardan Kurum sorumlu değildir. Kişisel hesabın bir başkasının eline geçmesi durumunda oluşabilecek sonuçlardan kişisel hesap sahibi sorumludur.

6.1.3.10. Kurum içi yazışmaları ve gizlilik dereceli verileri, kullanıcıların internet ortamında (sosyal medya, kişisel e-posta, anlık mesajlaşma uygulamaları, dosya paylaşım siteleri, forumlar vb.) paylaşması yasaktır.

6.1.3.11. Kurum hesaplarına ait kullanıcı adı ve şifrelerin paylaşılması yasaktır.

6.1.3.12. İnternette gezinirken reklam veya bilgi çalmak amaçlı (Örneğin: Tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın) aldatıcı resim ve içeriklere karşı dikkatli olunmalı, güvenli olmayan sitelere girilmemelidir.

6.1.3.13. İnternet erişimi Kurum genelinde tüm personele paylaşımlı olarak verilmekte olup, Kurum internet erişiminin verimli kullanılabilmesi adına Başkanlık gerekli gördüğü takdirde ilave güvenlik önlemi alma ve internet erişiminde kısıtlama yetkisine sahiptir.

6.1.3.14. Kuruma ait bilgisayarlar, güncellemeleri yapılmış, Kurum etki alanına dahil edilmiş, anti virüs ve ilgili güvenlik yazılımları yüklenmiş şekilde ağa dâhil edilir.

6.1.3.15. Kurum ağına erişim, ***Ağ Erişim Prosedürüne*** uygun olarak yapılır.

6.1.3.16. Kurum bilişim kaynaklarına ait iz kayıtları, ilgili yasa ve mevzuatlar gereğince tutulmakta olup söz konusu işlemler ***İz Kayıt Prosedürüne*** uygun gerçekleştirilir.

6.2. E-POSTA POLİTİKASI

6.2.1. Amaç

Kurum e-posta hesaplarının güvenli kullanımının sağlanması amaçlanmaktadır.

6.2.2. Kapsam

Bu politika Kurum e-posta hizmetini kullanan kullanıcıları kapsamaktadır.

6.2.3. Politika

6.2.3.1. Kurum e-posta hesabı; milletvekilleri, milletvekili yardımcı personelleri ve İdari Teşkilata bağlı çalışan personel için tanımlanır.

6.2.3.2. Kurum e-posta hesabı(…@tbmm.gov.tr) tanımlanan kullanıcılar, idari faaliyetlerinde bu hesabı kullanır.

6.2.3.3. Kurum e-posta adreslerinin kişisel işlemlerde(sosyal medya, forum, alışveriş, abonelik gerektiren vb. sitelerde) kullanılması yasaktır.

6.2.3.4. Kullanıcıların Kurum e-posta hesaplarından gönderdikleri, aldıkları veya sakladıkları e-postalar Kurumun bilgi varlığıdır. Gerekli durumlarda (idari soruşturma, hukuk davaları vb.) önceden haber vermeksizin bu e-posta hesapları denetlenebilir ve yargı organları ile paylaşılabilir.

6.2.3.5. E-posta kullanımına yönelik kota ve diğer sınırlamalar, ***E-Posta Kullanım Prosedürüne*** göre belirlenir.

6.2.3.6. Başkanlığın kullanıcılar ile e-posta yedeklerini paylaşma zorunluluğu bulunmamaktadır.

6.2.3.7. Kurum e-posta hesapları, İnsan Kaynakları Başkanlığınca personelin göreve başlatılması ile birlikte otomatik olarak geçici şifre verilerek oluşturulur. İlk kullanımda kullanıcı tarafından şifrenin değiştirilmesi zorunludur.

6.2.3.8. Kullanıcıların Kurum e-posta gruplarına, kişisel amaçlı e-posta göndermesi yasaktır.

6.2.3.9. Kurum e-posta hesapları; yasadışı, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik toplu e-posta, sahte, zincir ve iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postaların gönderilmesi için kullanılamaz. Bu tür bir e-posta alındığında ilk olarak SOME (some@tbmm.gov.tr) ekibine haber verilmesi ve ekip tarafından müdahale edilene kadar silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir.

6.2.3.10. Kullanıcılar, e-posta içeriğine kullanıcı adı ve şifre yazmamalıdır. Kullanıcı adı ve şifre talep edilen e-postalar alındığında ilk olarak SOME(some@tbmm.gov.tr) ekibine haber verilmesi ve ekip tarafından müdahale edilene kadar silinmemesi, yanıtlanmaması, iletilmemesi ve içeriğine tıklanmaması gerekmektedir. Başkanlık, kullanıcılardan hiçbir şekilde şifresini talep etmez.

6.2.3.11. E-posta gönderirken "Kime" ve "Bilgi" bölümlerine eklenen kişi listesi kontrol edilmeli ve içeriği dikkate alınarak sadece ilgili kişilere gönderilmelidir.

6.2.3.12. İdari Teşkilat birimlerine ait e-posta hesap ve grupları, ilgili birimlerin yazılı talebi doğrultusunda Başkanlık onayı ile oluşturulur.

6.2.3.13. Kullanıcı; Kurum e-posta hesabına ait içeriği, ilgisi bulunmayan kişilerle paylaşmayacağını, hizmet hakkının sadece kendisine ait olduğunu, kullanıcı adını ve şifresini başkasına kullandırmayacağını, başkası tarafından öğrenilme şüphesi olması halinde derhal değiştireceğini, aksi takdirde yapılan işlemin sorumluluğunun kendisine ait olacağını ve sorumluluktan kurtulamayacağını kabul eder.

6.2.3.14. Kullanıcı; e-posta içeriğinde ticari reklamlara, üyelik ile sağlanan yerli/yabancı destekleyici reklamlara ve bağlantılarına yer veremez. Ticari reklamlar ve haber duyuruları gibi istenmeyen mesajlar gönderemez.

6.2.3.15. Kullanıcıya ait e-posta hesabının siber güvenlik ihlalinde bulunması veya e-posta politikasına uyulmadığının tespiti halinde ilgili hesap Başkanlık tarafından geçici olarak kapatılır.

6.3. ANTİ-VİRÜS POLİTİKASI

6.3.1. Amaç

Bilgisayar ve sunucuların anti virüs programları ile korunması amaçlanmaktadır.

6.3.2. Kapsam

Bu politika Kurum etki alanında olan tüm bilgisayarları ve sunucuları kapsamaktadır.

6.3.3. Politika

6.3.3.1. Kurum etki alanında yer alan bilgisayar ve sunucularda anti virüs yazılımı kullanılacaktır.

6.3.3.2. Hiçbir kullanıcı herhangi bir sebepten dolayı anti virüs programının çalışmasını engelleyici faaliyette bulunamaz.

6.3.3.3. Anti virüs yazılımı düzenli aralıklarla güncellenecektir.

6.3.3.4. Anti virüs yazılımı, periyodik olarak bilgisayar ve sunucularda virüs taraması yapacaktır.

6.3.3.5. Bilgisayarlarda virüs tespit edildiğinde veya şüpheli durumlarda Başkanlığa haber verilmesi ve yetkili personel müdahale edene kadar bilgisayarın kullanılmaması gerekmektedir.

6.3.3.6. Virüs bulaşan bilgisayarlar temizleninceye kadar Kurum ağına bağlanmayacaktır.

6.3.3.7. Bilgisayarlarda kullanılacak CD/DVD, USB Bellek vb. depolama aygıtları ve internet üzerinden indirilen dosyalar virüs taraması yapmadan kullanılmamalıdır.

6.4. FİZİKSEL GÜVENLİK POLİTİKASI

6.4.1. Amaç

Kurumun bilgi varlıkları, ekipmanları ve altyapı cihazlarının fiziksel güvenliği ve yetkisiz erişimlerinin önlenmesi amaçlanmaktadır.

6.4.2. Kapsam

Kurumun bilgi varlıkları, ekipmanları ve altyapı cihazları kullanımını kapsamaktadır.

6.4.3. Politika

6.4.3.1. Kurum bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanacak ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları teşkil edilecektir.

6.4.3.2. Odalarda bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulacaktır.

6.4.3.3. Kurumun bilgi varlıkları, bilgisayar ve çevre birimleri (harici diskler, yazıcı, monitör, projeksiyon vb.), altyapı cihazlarını hasar / hırsızlık gibi oluşabilecek risklere karşı önlem almak ve güvenliği açısından uyarı yazıları yazmak personel ve birimin sorumluluğundadır.

6.4.3.4. Kritik bilgi varlıkları ile altyapı cihazları kilitli odalarda ve kabinetlerde muhafaza edilecektir.

6.4.3.5. Erişim yetkisi verilerek girilen alanların erişim yetkileri 3 aylık periyotlarla kontrol edilecektir.

6.4.3.6. Personel sadece kendi Kurum kimlik kartını kullanmakla yükümlüdür.

6.4.3.7. IP kameralarının kayıtları ***Kamera Prosedürüne*** uygun olarak tutulur.

6.5. VERİ MERKEZİ POLİTİKASI

6.5.1. Amaç

Kurum veri merkezlerinin güvenli ve sürdürülebilir şekilde işletilmesi amaçlanmaktadır.

6.5.2. Kapsam

Kurum veri merkezlerini kapsamaktadır.

6.5.3. Politika

6.5.3.1. Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.

6.5.3.2. Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı ortam izleme sistemi vasıtası ile gerekli tedbirler alınacaktır.

6.5.3.3. Sistem odası ortamı ideal sıcaklık seviyesinde tutulacaktır.

6.5.3.4. Sistem odalarına giriş çıkışlar ***Veri Merkezi Erişim Prosedürüne*** göre yapılacaktır.

6.5.3.5. Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunacaktır, yangın ve benzer felaketlere karşı koruma altına alınacaktır.

6.5.3.6. Sistem odalarında görüntü alınamaz.

6.5.3.7. Sistem odasında yiyecek içecek tüketmek ve sigara içmek yasaktır.

6.5.3.8. Sistem odalarının periyodik temizlik çalışmaları sistem odası personelinin eşliğinde yapılacaktır.

6.5.3.9. Sistem odalarına konulacak kritik cihazlar yedekli güç ünitelerine sahip olmalıdır.

6.6. AĞ CİHAZLARI YÖNETİM POLİTİKASI

6.6.1. Amaç

Kurumun ağ altyapısındaki, donanımı ve yazılımı zarara uğratan, tahrip edici, zedeleyici ve sağlıklı çalışmasını engelleyici hiçbir girişimde bulunulmaması; kaynakların verimli kullanılması amaçlanmaktadır.

6.6.2. Kapsam

Başkanlıkça yönetilen ağ altyapısı ve cihazları kapsamaktadır.

6.6.3. Politika

6.6.3.1. Kurumun ağ hizmetleri, Kurum faaliyetleri dışında ve yasalara aykırı faaliyetlerde bulunmak amacıyla kullanılamaz.

6.6.3.2. 5651 sayılı Kanun kapsamında, yetkili Başkanlık personeli tarafından, Kurum ağı ve cihazlarında oluşan trafik, kullanıcıların aldıkları hizmetler izlenebilecek, iz kayıtları tutulacak ve yönetilecektir.

6.6.3.3. Kurum ağına ve ağ cihazlarına yetkisiz erişim yapılamaz.

6.6.3.4. Başkanlık yönetiminde olmayan ağ cihazlarına ait tüm sorumluluk ilgili birime aittir.

6.6.3.5. Kurum ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için ağ altyapısı cihazları yedekli yapıda olacaktır.

6.6.3.6. Ağ cihazları yılda en az 1 defa açıklık yerel ağ tarama testlerinden geçirilerek zafiyetler tespit edilecek ve gerekli tedbirler alınarak güvenli hale getirilecektir.

6.6.3.7. Kurum ağı ve cihazları detaylı olarak takip edilecek ve izlenecektir.

6.6.3.8. Kabin yerleri, birimlerdeki ağ altyapısı kurulurken, internet erişiminin en verimli şekilde kullanılması, ağ altyapısı masraflarını ve kablo mesafelerine bağlı olarak veri kayıplarının en aza indirgenmesi dikkate alınarak belirlenir. Kabin ve kabin odalarıyla ilgili aşağıdaki kurallara uyulmak zorundadır;

6.6.3.8.1. Yetkisiz kişilerin kabin odalarına ve kabin içerisine erişmesi yasaktır.

6.6.3.8.2. Kabinleri besleyen elektrik prizlerine, sigortalara ve kesintisiz güç kaynağına yetkisiz müdahalede bulunulamaz.

6.6.3.8.3. Kabinlerin üzerine eşya, yakınına sıvı maddeler konulması ve kabinin güvenliğini bozacak her türlü durum için ortaya çıkabilecek sorunlardan ilgili birimler sorumludur.

6.6.3.8.4. Kurum ağ hizmetleri kaynaklarının herhangi bir amaçla kullanım hakkı, Başkanlık tarafından onay verilmeden üçüncü kişilere, özel veya tüzel kişilere verilemez.

6.6.3.8.5. Başkanlığın bilgisi dışında ağ kurmak, aktif-pasif cihazları ağa eklemek, kablosuz yayın yapmak ve ağ ile ilişkili yazılım/donanım kullanmak yasaktır.

6.6.3.8.6. Veri kablosu, sonlandırma ve aktarma işlemlerinde kullanılan bütün bileşenlerin (patch panel, veri prizi, patch kablolar vs.) uluslararası kablolama standartlarına uygun olarak kullanılması zorunludur.

6.7. UZAK BAĞLANTI POLİTİKASI

6.7.1. Amaç

Kurum bilişim kaynaklarına uzaktan erişim sağlayan Kurum çalışanları ve paydaşlarının kontrollü ve güvenli erişimleri amaçlamaktadır.

6.7.2. Kapsam

Bu politika Kurum bilişim kaynaklarına uzaktan erişim sağlayan Kurum çalışanları ve paydaşlarını kapsamaktadır.

6.7.3. Politika

6.7.3.1. Uzak bağlantı işlemi, Başkanlıkça belirlenen güvenli erişim bağlantı ve uygulamaları kullanılarak yapılır. İzinsiz uzak bağlantı yapılması yasaktır.

6.7.3.2. Uzak bağlantı talepleri ***Uzak Bağlantı Prosedürüne*** göre gerçekleştirilir.

6.7.3.3. Uzak bağlantı yapmasına izin verilen kullanıcıların hesap bilgilerini başkalarıyla paylaşması yasaktır.

6.7.3.4. BGYS politikalarına aykırı olmamak koşulu ile uzak bağlantı talep eden birim bu durumu ihtiyaç duyduğu süreyi de belirterek yazılı olarak Başkanlığa bildirir

6.7.3.5. Başkanlık gerekli gördüğü durumlarda herhangi bir uyarıda bulunmaksızın uzak bağlantı erişimlerini kesme hakkına sahiptir.

6.8. ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

6.8.1. Amaç

Kurumun bilgi teknolojilerine ve bilgi varlıklarına üçüncü tarafların ulaşılması durumunda güvenliğin sağlanması amaçlanmaktadır.

6.8.2. Kapsam

Bu politika paydaşları kapsamaktadır.

6.8.3. Politika

6.8.3.1. Paydaşlar ile bilişim hizmetleri kapsamında bilgi varlıklarına müdahale, test, bakım onarım vb. süreçlerin gerçekleştirilmesi için gizlilik sözleşmeleri veya iş birliği protokolü yapılır.

6.8.3.2. Paydaşlara, Kurumun bilgi teknolojileri sistemlerine veya bilgi varlıklarına erişim ihtiyacı olması halinde kısıtlı yetki verilecektir.

6.8.3.3. Paydaşların, Kurumun bilgi teknolojileri sistemlerine veya bilgi varlıklarına uzaktan erişim ihtiyacı durumunda ***Uzak Bağlantı Prosedürüne*** göre yetki verilecektir.

6.8.3.4. Paydaşlar, Kurumun bilgi teknolojisi sistemlerinin bulunduğu fiziksel ortamına Kurum personeli refakati olmadan giremez.

6.9. KRİPTOGRAFİK KONTROLLER POLİTİKASI

6.9.1. Amaç

Bilgi varlıklarının saklandığı sistemler üzerindeki verilere erişim güvenliği ve bilgi varlıklarının transfer gizliliğinin korunması amaçlanmaktadır.

6.9.2. Kapsam

Bu politika kullanıcı ve bilişim kaynaklarını kapsamaktadır.

6.9.3. Politika

6.9.3.1. Gizli olarak ifade edilen bilgi varlıklarının paylaşımında güçlü şifreleme algoritmaları kullanılacaktır. Bilgi varlıkları paylaşılmadan önce sıkıştırma programı (winrar, winzip v.b.) kullanılarak şifrelenecektir.

6.9.3.2. Kurumun sağladığı tüm servisler (e-posta, ftp, web vb.) güvenilir sertifika doğrulaması yapılarak hizmet verecektir.

6.9.3.3. Kurum etki alanında yer alan ve web servislerine erişim sağlayan cihazlarda Kurum sertifika otoritesi tarafından imzalanan kök sertifika bulunacaktır.

6.9.3.4. Kurum şifreleme algoritması güncel ve güçlü algoritmalar kullanılarak yapılacaktır.

6.10. KABUL EDİLEBİLİR KULLANIM POLİTİKASI

6.10.1. Amaç

Kurum bilişim kaynaklarını kullanırken gizlilik, bütünlük ve erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarını personele bildirmeyi amaçlamaktadır.

6.10.2. Kapsam

Bu politika idari teşkilat birimlerini, personeli ve paydaşları kapsamaktadır.

6.10.3. Politika

6.10.3.1. Kurum çalışanları, kendilerine tahsis edilmiş olan bilişim kaynakları ve ortak kullanım alanları (dosya paylaşım sistemi, e-posta hesabı vb.) üzerinde görevi dışında hiçbir veri, bilgi, belge, resim veya telif hakkı içeren elektronik dosya bulunduramaz. Bu cihazlar ile üzerindeki tüm veriler Kuruma aittir ve iş amaçlı kullanım için verilmiştir.

6.10.3.2. Kurum, BGYS politikalarına aykırı olayların tespit edildiği durumlarda herhangi bir uyarıda bulunmadan kullanıcıya tahsis edilen cihazları geri alma ve üzerindeki verilere erişimi kısıtlama hakkına sahiptir.

6.10.3.3. Kurum çalışanları, Kuruma ait verilerin, bilgi, belge ve bilişim kaynaklarının gizliliğine dikkat etmek zorunda olup izinsiz olarak kopyalanması, çoğaltılması, değiştirilmesi ve paylaşılması yasaktır.

6.10.3.4. Kullanıcılar, kendilerine tahsis edilmiş bilişim kaynağının erişim bilgilerini ve güvenliğini korumakla sorumludur, bu bilgilerin paylaşılması yasaktır.

6.10.3.5. Kullanıcıların kendisine tahsis edilmiş veya yetkilendirilmiş bilişim kaynağına Kurum tarafından lisanslandırılmış olmayan veya üretici firması tarafından kopya edilmesi yasaklanmış bir yazılımı kurması, kullanması veya kopyalaması yasaktır.

6.10.3.6. Gizli dokümanlara erişim yetkisi bulunan kullanıcı, doküman içeriğindeki bilginin korunmasından sorumludur.

6.10.3.7. Kullanıcı, Kuruma ait gizli olsun ya da olmasın bilgi, belge veya veri bulur ise bu durumu SOME birimine bildirmekle yükümlüdür.

6.10.3.8. Kullanıcılar, "Gizli" ibareli belgeleri kilitli dolaplarda muhafaza edecektir.

6.10.3.9. Kullanıcıların, Kurum tarafından kendisine tahsis edilen cihazları, herhangi bir kimseye (aile bireyleri vb.) kullandırması veya paylaşması yasaktır.

6.10.3.10. Kurum bilişim kaynaklarından hizmet alan kullanıcılar, ***Şifre Prosedürüne*** göre belirlenmiş güçlü ve kompleks yapıda şifreler kullanmakla sorumludur.

6.11. TEMİZ MASA TEMİZ EKRAN POLİTİKASI

6.11.1. Amaç

Kullanıcıların mesai saatleri içinde veya dışında görevini yaparken edindiği veya kullandığı bilgi, belge ve verilere yetkisiz kişilerce erişimi engellemek veya uygunsuz kullanımı sonucunda oluşabilecek riskleri ortadan kaldırmak amaçlanmaktadır.

6.11.2. Kapsam

Bu politika kullanıcıları kapsamaktadır.

6.11.3. Politika

6.11.3.1. Kullanıcı çalışma masasından ayrıldığında basılı doküman ya da taşınabilir depolama aygıtları üzerinde tutulan bilgiler, güvenli ortamlarda (çelik kasa, kilitli dolap ve çekmeceler vb.) saklanacaktır.

6.11.3.2. Yetkisiz erişimlere karşı her türlü faks, fotokopi, yazıcı vb. cihazlar üzerinde belge, doküman bırakılmayacaktır.

6.11.3.3. Kullanıcılar, Kuruma ait bilgi içeren sistemleri şifresiz kullanmayacak ve ekran başından kısa süreli de olsa ayrılırken ekran kilidini aktif hale getirecektir. Kullanıcı adı ve şifreler herkesin kolayca ulaşabilecekleri yerlerde bulundurulmayacaktır.

6.11.3.4. Elektronik ortamda bulunan verilerin ve cihazların imhası 5651 sayılı Kanunda belirtilen süreler dikkate alınarak ***İmha Prosedürüne*** göre yapılır.

6.11.3.5. Kuruma ait resmi evraklar, veri dokümanları, şartnameler, faturalar gibi dokümanlara kurum mevzuatına göre arşiv ve imha prosedürleri uygulanır, bu dokümanlar müsvedde olarak kullanılmaz.

6.12. MOBİL CİHAZ POLİTİKASI

6.12.1. Amaç

Kuruma ait mobil cihazların güvenli kullanımı ve yönetimi amaçlanmaktadır.

6.12.2. Kapsam

Kuruma ait mobil ve taşınabilir cihazları kapsar.

6.12.3. Politika

6.12.3.1. Mobil cihazlar (cep telefonu, dizüstü bilgisayar, USB bellek, harici disk, tablet, sim kart vb.) ilgili kullanıcıya veya birime zimmetlenecektir.

6.12.3.2. Kullanıcı/birim zimmeti yapılan cihazın BGYS politika ve prosedürlerine uygun olarak kullanımından sorumludur.

6.12.3.3. Kuruma ait mobil cihazlara yetkisiz müdahaleyi önlemek kullanıcının/birimin sorumluluğundadır.

6.12.3.4. Kurum telefon hatları ve mobil cihazlar üzerinden uygunsuz, müstehcen, rahatsız edici materyaller ve başkalarına iftira, karalama mahiyetinde iletişim kurmak, mesajlar yayınlamak ve paylaşmak yasaktır.

6.12.3.5. Kullanıcı, mobil cihazlarda ne tür bilgiler saklandığının farkında olmalı ve Kuruma ait bilgilerin mobil cihazlar üzerinde güvenliğini sağlamalıdır.

6.13. VERİ TABANI GÜVENLİK POLİTİKASI

6.13.1. Amaç

Kurumun veri tabanı sistemlerinin güvenli kullanımı ve yönetimi amaçlanmaktadır.

6.13.2. Kapsam

Başkanlığın sorumluluğundaki veri tabanı sistemlerini kapsar.

6.13.3. Politika

6.13.3.1. Veri tabanı sunucularına, Başkanlığın yetkilendirdiği kişiler ve sistemler dışında erişim yapılması yasaktır. Erişim istekleri ***Ağ Erişim Prosedürüne*** göre yapılır.

6.13.3.2. Veri tabanında kritik verilere erişim işlemlerinin iz kayıtları tutulacak olup bu kayıtlara Başkanlığın yetkilendirdiği kişi ve sistemler dışında erişim yapılması yasaktır.

6.13.3.3. Veri tabanı yedekleri ***Yedekleme Prosedürüne*** göre alınacaktır.

6.13.3.4. Veri tabanı sunucuları fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulacaktır.

6.13.3.5. Veri tabanı bulunan medyalar (harici disk, USB bellek vb.) Kurum dışına çıkarılmayacaktır.

6.13.3.6. Veri tabanı sunucularının kaynakları (cpu, ram, disk, ağ trafiği vb.) düzenli olarak kontrol edilecektir.

6.13.3.7. Paydaşların veri tabanlarına erişimi, Başkanlık onayıyla Kurum bünyesinde ve personelin gözetiminde yapılabilir.

6.13.3.8. Veri tabanı sistemleri envanteri dokümante edilir ve bu envanterden sorumlu personel tanımlanır.

6.13.3.9. Paydaşların çalışmaları için test veri tabanı oluşturulup ***Ağ Erişim Prosedürüne*** göre izinler verilir.

6.13.3.10. En üst düzey veri tabanı yöneticiliği sadece Başkanlık tarafından yetkilendirilmiş kullanıcılara verilir.

6.14. YAZILIM TEMİNİ VE GELİŞTİRME POLİTİKASI

6.14.1. Amaç

Kurumun yazılım temini ve geliştirme ihtiyacının güvenli yönetilmesini amaçlamaktadır.

6.14.2. Kapsam

İdari teşkilat birimlerinin ihtiyaçları doğrultusunda yazılım temini ve geliştirme sürecini kapsar.

6.14.3. Politika

6.14.3.1. Yazılım geliştirmede, ihtiyaç analizi, tasarım, geliştirme, deneme ve onaylama safhalarını içeren iş planı kullanılacaktır.

6.14.3.2. Siber Güvenlik Ekibince yapılan güvenlik testlerinden geçmemiş yazılımların (geliştirilen, satın alınan veya revize edilen) Kurum içerisinde kullanılması yasaktır.

6.14.3.3. Kurum içerisinde geliştirilen yazılımlar ***Güvenli Yazılım Geliştirme Prosedürü*** uygun olacaktır.

6.14.3.4. Kuruma ait yazılımlar ***Varlık Envanteri Listesine*** eklenecek ve takip edilecektir.

6.14.3.5. Kurum tarafından hizmete sunulan tüm uygulamalardan iz kayıtları alınıp alınmadığı düzenli aralıklarla kontrol edilecektir.

6.14.3.6. Yeni yazılımların sürüm takibi ve dağıtımı kontrol altında tutulmalıdır.

6.15. VERİ ARŞİVLEME VE YEDEKLEME POLİTİKASI

6.15.1. Amaç

Kurum bilişim kaynakları üzerinde oluşturulan, kullanılan ve devamlılığı gerekli görülen verilerin saklanması ve muhafazası konusunda gerekli önlemleri almak amaçlanmaktadır.

6.15.2. Kapsam

Arşivleme, Başkanlığın kontrolünde olan verilerin(veri depolama ve sunucularda), güvenli olarak saklanması, gerektiğinde kullanıma açılması ve ihtiyaç sonunda silinmesine ilişkin gerekli yöntemleri kapsar.

Yedekleme, Başkanlık tarafından kurulmuş olan fiziksel ve sanal sunucuların veri yedeklerini kapsar.

6.15.3. Politika

6.15.3.1. Başkanlık bünyesinde kullanılan sunucu ve sistemlerin düzenli aralıklarla ve teknik imkanlar dahilinde ***Yedekleme Prosedürüne*** göre yedekleri alınır.

6.15.3.2. Başkanlığın kontrolünde olan verilerin arşiv işlemleri ***Arşiv Prosedürüne*** göre yapılır.

6.15.3.3. Başkanlık yönetiminde olmayan cihaz ve sistemlere ait verilerin yedekleme ve arşiv işlemlerinden kullanıcı sorumludur.

6.15.3.4. Veri yedeği alınan sunucu ve sistemler düzenli aralıklarla raporlanacaktır.

6.15.3.5. Yedekleme prosedürü dışında olan sistem ve cihazlarla ilgili herhangi bir veri kurtarma talebinde bulunulamaz.

6.16. OLAY YÖNETİM POLİTİKASI

6.16.1. Amaç

Bilgi güvenliği olaylarının kayıt altına alınması ve yönetilmesini amaçlamaktadır.

6.16.2. Kapsam

Bu politikanın uygulanmasından kullanıcılar sorumludur.

6.16.3. Politika

6.16.3.1. Kuruma ait bilgi ve belgelerin gizliliğinin, verilerin tamamı veya bir kısmının değiştirilmesi, bozulması ve yetkisiz kişilerce erişilmesi durumlarında oluşan güvenlik ihlali, kullanıcı tarafından kayıt altına alınır ve en kısa sürede Başkanlık Siber Olaylara Müdahale Ekibine (SOME) (some@tbmm.gov.tr) bildirilir.

6.16.3.2. Bilgi güvenliği olaylarına ***Olay Yönetimi Prosedürüne*** göre müdahale edilir.

6.16.3.3. Bilgi güvenliği olayları cezai ve hukuki mesuliyetle sonuçlanabilir. Kurum, bu tür olayların olduğu durumları araştırır ve eğer suç oluştuğundan şüphe duyarsa disiplin yönetmeliğini uygular ve/veya adli makamlara ihbarda bulunabilir.

6.16.3.4. SOME, bilgi güveliği ihlali tespiti veya bildirimi sonrasında ilgili bilişim kaynağında inceleme ve müdahale etme yetkisine sahiptir. Ayrıca olayları analiz ederek tekrarlanmaması için düzeltici ve önleyici tedbirler alınması sağlar.

6.17. SUNUCU YÖNETİMİ VE GÜVENLİĞİ POLİTİKASI

6.17.1. Amaç

Başkanlık tarafından yönetilen sunucuların yönetim ve güvenliğinin sağlanması amaçlanmaktadır.

6.17.2. Kapsam

Bu politika Başkanlığın yönetimindeki sunucuları kapsamaktadır.

6.17.3. Politika

6.17.3.1. Kurum bünyesindeki tüm sunucuların yönetiminden sadece yetkilendirilmiş kullanıcı sorumludur.

6.17.3.2. Sunucu ve sistem yönetimi için erişim talepleri ***Ağ Erişim Prosedürüne*** göre yapılacaktır.

6.17.3.3. Sunuculara Başkanlığın yetkilendirdiği kişiler dışında erişim yapılamaz.

6.17.3.4. Sunucuların kaynakları (cpu, ram, disk, ağ trafiği vb.) izlenecek ve düzenli olarak raporlanacaktır.

6.17.3.5. Sunucular yılda en az 1 defa açıklık tarama testlerinden geçirilerek gerekli tedbirler alınacaktır.

6.17.3.6. Dosya sunucusu(ortak paylaşım alanı) üzerinde, kişisel dosyaların(kişisel bilgisayar, cep telefonu yedekleri, film, müzik vb.) bulundurulması ve yedeklenmesi yasaktır. Başkanlık tarafından yapılan kontrollerde tespit edilmesi halinde dosyaların silinmesini ilgili kullanıcı kabul etmiş olur.

6.17.3.7. Sunucularda saldırı yüzeyini genişletecek şekilde 3. parti programların kullanılması uygun değildir. Bu tür programlara ihtiyaç duyulması halinde SOME ekibinden onay alınması gerekmektedir.

6.17.3.8. Sunucu kurulumu ve konfigürasyonu, ***Sunucu Kurulum ve Yapılandırma Prosedürü*** uygun şekilde yapılır.

6.17.3.9. Yeni yayınlanan güvenlik yamaları düzenli olarak kontrol edilir, gerekli testler yapıldıktan sonra sunuculara yüklenir. Bu işlemler ***Değişim Yönetimi ve Kapasite Prosedürü*** göre yapılır.

6.17.3.10. Sunucular, ***Yedekleme Prosedürüne*** uygun şekilde yedeklenir.