Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
00	-	İlk Yayın
01	05.09.2019	Politika numarası değiştirildi.

1. AMAÇ

Bu doküman bilişim ortamlarındaki Virüs, Solucan, Truva Atı ve diğer zararlı kodlara ve saldırılara karşı Bilecik Şeyh Edebali Üniversitesi Bilgi İşlem Daire Başkanlığı kuruluş politikasını tanımlamaktadır.

2. KAPSAM

Bu politika, zararlı kodların bulaştığı tüm bilişim ortamlarını, elektronik iletişim medyasını ve depolama ortamlarını kapsar. Politika metninde Bilecik Şeyh Edebali Üniversitesi Bilgi İşlem Daire Başkanlığı ibaresi BSEÜ-BİDB olarak anılacaktır.

3. UYGULAMA

- Tüm bilgisayarlar, BSEÜ-BİDB Yönetimi tarafından onaylanmış en son antivirüs yazılımları ile koruma altına alınmalıdır.
- Bilinmeyen ve şüpheli bir kaynaktan gelen e-posta mesaj ve ekleri açılmamalıdır.
- Bilgisayarlarda kullanılan tüm taşınabilir medya ortamları (disket sürücü, Flash ROM, CD-ROM vs.) kullanılmadan önce virüs taramasına tabi tutulmaldır.
- Tüm e-posta sunucuları için antivirüs koruma yazılımı yüklenmeli; tüm e-posta ve ekleri antivirüs taramasından işlem öncesi geçirilmelidir.
- Antivirüs yazılımının tüm güncel imzaları merkezi olarak antivirüs firmasının onaylı sunucusundan otomatik olarak yüklenmeli ve ilgili sunuculara dağıtımı yapılmalıdır.
- İnternet üzerinden kaynağı belli olmayan web sitesinden yazılım yüklemesi yapılmamalıdır.
- BSEÜ-BİDB Sistem Uzmanı tarafından siber saldırılarla mücadele için kullanılması yasaklanan ve kurum içinde duyurulan yazılım ve bileşenleri hiçbir personel tarafından kullanılmamalıdır.
- BSEÜ-BİDB kuruluş ağına bağlanması gerekli olan BSEÜ-BİDB dışı istemci ve taşınabilir bilgisayarları ağa DMZ (Demilitarized Zone) ile bağlanmalıdır.
- BSEÜ-BİDB personeli, e-posta veya başka yollarla kendilerine gelen ve kendilerinden istenen parola, kullanıcı kimlik veya gizli bilgileri iletmemeli ve böyle durumlar olursa bunu BSEÜ-BİDB Sistem Uzmanına ivedilikle bildirmelidir.
- BSEÜ-BİDB personeli, kendi bilgisayarlarından BSEÜ-BİDB tarafından kurulmuş olan antivirüs ve/ya SPAM koruma yazılımlarını devre dışı bırakamaz veya kaldıramaz.
- BSEÜ-BİDB bilişim ağına etkileşimli olarak bağlanacak herhangi bir bilgisayar sisteminin virüs, truva atı, solucan veya diğer zararlı kodlardan muaf olduğu tespit edildikten sonra bağlantısı gerçekleştirilmelidir.
- BSEÜ-BİDB ağı ve önemli sunucu bileşenleri için Ağ ve Sunucu Saldırı Tespit sistemleri devreye alınmalıdır.

- Siber saldırı olması durumunda BSEÜ-BİDB güvenlik duvarı bağlantıları engellemelidir. Durum hakkında bilgi kurum Siber Olaylara Müdahale Ekibi(SOME) birim yetkilisine bildirilmelidir.

4. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında Disiplin Prosedürü hükümleri uygulanır.

5. İLGİLİ DOKÜMANLAR

- AĞ ve ERİŞİM GÜVENLİĞİ POLİTİKASI BGYS.PLT.02
- ANTİVİRÜS POLİTİKASI BGYS.PLT.04
- DİSİPLİN PROSEDÜRÜ BGYS.PRS.14