EKOGLOBAL İSG İŞ SAĞLIĞI GÜVENLİĞİ RİSK YÖNETİMİ HİZMETLERİ EĞİTİM MÜHENDİSLİK MÜŞAVİRLİK SAN. VE TİC. LTD. ŞTİ

TEDARİKÇİ İLİŞKİLERİ İÇİN BİLGİ GÜVENLİĞİ POLİTİKASI

Hazırlayan	Onaylayan

1. AMAÇ

Bu bilgi güvenliği politikasının amacı şirketin ve iş stratejileri doğrultusunda müşterilerinin bilgi varlıklarını iç veya dış, bilerek veya bilmeyerek oluşabilecek bütün tehditlere karşı korumaktır. Bu politikanın uygulanması, rekabet avantajı sağlamak için bilgi varlıklarımızın gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için önemlidir.

Uygun risk değerlendirmesi yoluyla bilgi varlıklarının değerini tespit etmek ve bu varlıkların açıklarını ve onları riske maruz bırakabilecek tehditleri anlamak.

Bir Bilgi Güvenliği Yönetim Sistemi (BGYS) tasarlama, uygulama, bakım ve iyileştirme yoluyla riskleri yönetmek, kontrol etmek ve kabul edilebilir bir seviyeye indirmek.

Eko Global İsg'nin müşterileriyle olan sözleşme yükümlülüklerine uymak.

Eko Global İsg'in kurumsal direktiflerine uymak.

ISO 27001 de dahil olmak üzere, güvenlik hedefleri ve kontrolleri çerçevesinde bilgi güvenliği taahhüdünü gerçekleştirmek.

2. KAPSAM

Tedarikçi ilişkilerinde bilgi güvenliğinin korunması için uyulması gereken kuralları kapsar.

3. SORUMLULAR

3.1. Prosedürün Kullanıldığı Birimler: Eko Global İsg Çalışanları, Eko Global İsg Tedarikçi Sözleşmeli İş Ortakları.

3.2. Prosedürün Yürütülmesi için Sorumlular: Eko Global İsg Çalışanları, Eko Global İsg Tedarikçi Sözleşmeli İş Ortakları.

3.3. Tedarikçinin tüm personeli bu güvenlik politikasını korumak için prosedür ve kurallara uyacaktır.

3.4. Tedarikçinin tüm personeli algılanan güvenlik zayıflıklarını rapor edecektir.

3.5. Tedarikçinin tüm personeli, ilgili güvenlik politikalarına uymak için, Eko Global İsg'nin internet sitesindeki en son sürümlerine bakarak güvenlik politikaları ile ilgili bilgilerini güncel tutmakla yükümlüdür.

4. YÜKÜMLÜLÜKLER

Eko Global İsg bilgi güvenliği politikası aşağıdaki maddeleri sağlamak üzere hazırlanmıştır: Bilgi yetkisiz erişime karşı korunacak.

4.1. Bilginin gizliliği muhafaza edilecek.

4.2. Bilgi bilerek veya bilmeyerek yetkisiz kişilere ifşa edilmeyecek.

4.3. Bilginin bütünlüğü yetkisiz değişikliğe karşı korunacak.

4.4. Gerektiğinde yetkili kullanıcılar bilgiye erişebilecek.

4.5. Düzenleyici ve yasal gereklilikler yerine getirilecek.

4.6. İş sürekliliği planları oluşturulacak, sürdürülecek ve test edilecek.

4.7. Şirket içinde çalışan tüm tedarikçi çalışanlarına bilgi güvenliği eğitimi verilecek.

4.8. Tüm bilgi güvenliği ihlal şüpheleri raporlanacak ve incelenecek.

5. TANIMLAR

1. İş ortağı: Tedarikçinin Eko Global İsg kaynaklarına erişen personeli/çalışanı. Sözleşmeli personel, stajyerler, geçici personel, dış danışmanlar ve Eko Global İsg dahilinde çalışan üçüncü parti personel buna dahildir.

2. Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliği oluşturmak, uygulamak, işletmek, izlemek, gözden geçirmek, korumak ve artırmak için, iş riski yaklaşımına dayalı genel yönetim sisteminin bir parçasıdır. Yönetim sistemi; organizasyon yapısını, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, süreçleri ve kaynakları içerir.

3. Bilgi Güvenliği Olayı: İş süreçlerini riske atma ve bilgi güvenliğini tehdit etme olasılığı yüksek bir tek veya bir dizi istenmeyen veya beklenmeyen bilgi güvenliği olayı.

6. UYGULANABİLİRLİK

Tedarikçilerin şirket içinde çalışan veya şirket bilgi kaynaklarına uzaktan erişebilen bütün personeli bu politikayı uygulamakla yükümlüdür. Bu politikanın kapsamı Ek-A' da listelenmiştir.

7. HEDEFLER

7.1. Şirketin müşteri bilgilerini korumak

7.2. Şirketin bilgi varlılarını korumak

7.3. Bilginin paylaşılmasına ihtiyaç duyulan durumlarda iş ortaklarına ve müşterilere güven sağlamak

7.4. Planlanmamış kesinti riskini en aza indirmek amacıyla ağı ve altyapı genelinde sistem çalışma süresini izlemek, korumak ve optimize etmek

7.5. Uyumlu olmayan (onaylanmamış) yazılım kurulumunu engellemek

7.6. Güvenlik olaylarına göre güvenlik politikalarını ve prosedürlerini formüle etmek ve gözden geçirmek

7.7. Tüm kullanıcılarda farkındalık yaratmak, bilgi güvenliği eğitimi vermek ve bu eğitimlerin etkinliğini ölçmek

8. **OLAY RAPORLAMA**

   Tedarikçinin tüm personeli güvenlik olaylarını "Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü"ne göre raporlamaktan sorumludur.

9. **İLETİŞİM**

   Bu politika dokümanı Tedarikçi tarafından tüm paydaşlarına uygun, erişilebilir ve kullanıcı tarafından anlaşılabilir bir formda hazır bulundurulmalıdır.

10. **GÖZDEN GEÇİRME**

    Bu politika, politikanın şirketin iş amaçlarına uygunluğunu ve müşterilerine hizmet etme kabiliyetini sağlamak amacıyla, periyodik olarak (en az yılda bir kere) ve Eko Global İsg içinde yapılan değişiklikler gerektirdiğinde gözden geçirilecektir.

EK: A

KAPSAM:

Bu BGYS aşağıdakileri kapsar:

1. Eko Global İsg'ye ait tesislerde çalışan, ortak tesisleri paylaşan ve Eko Global İsg lokasyonlarındaki bilgi varlıklarına erişimi olan tüm tedarikçi çalışanları, ortakları, müteahhitleri.
2. Eko Global İsg'nin müşteri lokasyonlarında çalışan ve Eko Global İsg'nin bilgi varlıklarına erişimi olan tüm tedarikçi çalışanları ve ortakları.
3. Eko Global İsg ağına bağlanacak yeni ekipman gerektiren tüm uygulamalar ve işlevler.
4. Ağı idare eden ve yöneten BT ekipleri.
5. Eko Global İsg bilgi sistemlerinin bağlı olduğu bütün (mevcut ve gelecek) Eko Global İsg ağı.
6. Yukarıda adı geçen bütün ağlara bağlı ekipman.
7. Yukarıda adı geçen ağlardan geçen bütün veriler.

Aşağıdakiler de dahil olmak ancak bunlarla sınırlı olmamak üzere:

1. Kullanıcı ağı
2. DMZ ağı
3. Internet ağı
4. Tüm omurga servisleri, switchler, ADSL vs.
5. Uzaktan bağlantı ile çalışan kullanıcılar.

EK: B

A. Kabul Edilebilir Kullanım

Genel olarak, aşağıdaki faaliyetler Eko Global İsg tesislerinde bilgi varlıklarının kullanımı ile ilgili kabul edilebilir kullanım şartlarıdır. Eko Global İsg'de sorumlu oldukları işleri yerine getirirken Eko Global İsg bilgi varlıklarını kullanan tedarikçi çalışanları ve ortakları da bu şartlara bağlıdır.

1. Sistem ve uygulamalara giriş için güçlü şifreler kullanın.
2. Masanızın üzerinde yer alan gizli belgeleri koruyarak masanızı ve ekranınızı temizleyin.
3. Eko Global İsg ve müşterilerinin gereksinimlerine göre dokümanlarınızı sınıflandırın.
4. Eko Global İsg ağında veya sistemlerinde kullanmadan önce, kapıdan girişte elektronik medyanızı beyan edin.
5. Gerekli veri ve yazılımlarınızın sık sık yedeğini alın.
6. Sisteminizdeki anti-virus yazılımının güncel olduğundan emin olun.
7. Virüs olabilecek şüpheli dosya ve programlara karşı her zaman dikkatli olun.
8. İndirdiğiniz dosyaları açmadan önce bir virüs programı ile tarayınız.
9. Gizli bilgi içeren yazıcı çıktılarını hemen yazıcıdan alın.
10. Eko Global İsg tarafından girişte verilen kartları görülebilir şekilde her zaman boynunuzda taşıyın.
11. Eko Global İsg tesislerinde misafirlerinize sürekli eşlik ediniz.
12. Lisanslı yazılım kullanın ve yazılım üreticisinin yazılım kullanım sözleşmesine uyun.
13. Resmi internet ve e-posta sistemlerini sadece iş amaçlı kullanın.
14. Telefonda herhangi bir bilgi paylaşmadan önce lütfen arayanın kimliğini ve talebinin meşru olup olmadığını doğrulayın.
15. Gizli veri içeren sistemlerde klasörlere erişim denetimi uygulayın.
16. Basılı gizli belgeleri parçalayarak imha edin.
17. Elektronik medya ve cihaz içeriklerini Eko Global İsg İmha prosedürüne göre imha edin.
18. Eko Global İsg tesisleri dışında, (eğer varsa) Eko Global İsg tarafından sağlanan notebook ve mobil cihazlarınızı başıboş bırakmayın.
19. Bilgi güvenliği politikaları ile ilgili bilginizi güncel tutun ve bunlara uyun.
20. Bütün güvenlik ihlallerini ve olası güvenlik açıklarını ……. adresine raporlayın.

B. Kabul Edilemez Kullanım

Genel olarak aşağıdaki faaliyetler yasaktır. Eko Global İsg bilgi varlıklarını kullanan tedarikçi çalışanları ve ortakları, Eko Global İsg' deki meşru iş sorumlulukları süresince, daha önceden Eko Global İsg'den onay almış olma kaydıyla, bu yasaklardan muaf tutulabilir. Tedarikçi çalışanları ve ortakları, Eko Global İsg'nin kaynaklarını kullanırken, hiçbir koşulda yerel ve uluslararası yasaları çiğneyecek bir faaliyette bulunamaz. Aşağıdaki liste ayrıntılı olmamakla beraber kabul edilemez kullanım kategorisine giren faaliyetler için bir çerçeve oluşturmaktadır.

11. Sistem ve Ağ Faaliyetleri

Aşağıdaki faaliyetler istisnasız yasaktır:

1. Korsan veya Eko Global İsg'de kullanım için uygun şekilde lisanslanmamış yazılımların kurulumu veya dağıtımı da dahil olmak, ama bunlarla sınırlı kalmamak üzere; herhangi bir kişi veya şirketin telif hakkı, ticari sır, patent veya diğer fikri mülkiyet veya benzer yasalar ve yönetmelikler ile koruma altına alınmış haklarının ihlali.
2. Dergi, kitap ve diğer telif haklı kaynaklardaki fotoğrafların, telif haklı müziklerin sayısallaştırılması ve dağıtılması da dahil olmak ama bunlarla sınırlı kalmamak üzere; tüm telif haklı materyallerin yetkisiz kopyalanması, Eko Global İsg veya son kullanıcının geçerli bir lisansı olmayan telif haklı bir yazılımın kurulumu kesinlikle yasaktır.
3. Ağa veya sunucuya kötü amaçlı yazılım bulaştırma (ör. virüs, solucan, Truva atı, e-posta bombası vb.)
4. Kullanıcı bilgisayarlarına oyun, telif haklı şarkı, film, pornografik materyal gibi herhangi bir yasaklı materyal ve yazılımın izinsiz kurulumu ve kopyalanması kesinlikle yasaktır.
5. Evde çalışırken aile bireyleri de dahil olmak üzere, şifrelerinizi başkalarına vermek veya hesap bilgilerinizin başkaları tarafından kullanılmasına izin vermek.
6. Ağ haberleşmesinde güvenlik ihlali veya kesintiye sebep olmak. Günlük görevlerinin kapsamı içinde tanımlı bir iş olmamasına rağmen çalışan veya ortağın amaçlanan alıcı olmadığı veriye erişmesi veya açıkça yetki verilmemiş sunucu veya hesaba giriş yapması gibi konular bunlarla sınırlı kalmamak kaydıyla güvenlik ihlalleridir. Bu bölüm kapsamında "bozulma" (bunlarla sınırlı kalmamak üzere) network sniffing, pingedfloods, packetspoofing, denial of service, ve kötü amaçlı sahte yönlendirme bilgileri gibi gibi faaliyetleri ifade eder.

7. Çalışanın veya iş ortağının normal görevinin bir parçası olmadığı halde, çalışanın veya iş ortağının sistemine gönderilmemiş olan bir veriyi ağ üzerinde yakalayacak her tür ağ izleme işini yürütmek.
8. Kullanıcı kimlik doğrulaması veya herhangi bir bilgisayar, ağ veya hesap güvenliğinin çevresinden dolaşmak.
9. Eko Global İsg üst yönetiminin yazılı izni olmadan herhangi bir Eko Global İsg çalışanı, projesi veya ürünü ile ilgili Eko Global İsg dışında bilgi paylaşmak veya yayınlamak.

12. E-posta, Internet ve Haberleşme Faaliyetleri

1. Özellikle bu tür materyalleri talep etmemiş kişilere istenmeyen e-posta iletileri, önemsiz posta veya diğer reklam iletileri (spam) gönderimi.
2. Eko Global İsg politikaları ile yasaklanmış internet sitelerine erişim.
3. Kullanılan dil, mesaj sıklığı veya boyutu yoluyla e-posta, telefon veya çağrı ile her türlü taciz.
4. E-posta başlık bilgilerinin yetkisiz kullanımı veya sahte başlık kullanımı.
5. Taciz etmek veya cevap toplamak amacıyla kendi kullanıcı hesabı dışında başka bir e-posta adresi talep etmek.
6. Zincir posta veya benzer piramit yapıda posta oluşturmak veya iletmek.
7. İş ile ilgisi olmayan benzer veya aynı e-posta mesajını çok sayıda kullanıcıya göndermek.
8. Kullanıcılar, Eko Global İsg bilgisayar sistemleri üzerinde yarattığı, depoladığı, gönderdiği veya aldığı her şey için gizlilik hakkından feragat eder. Eko Global İsg önceden haber vermeden e-postaları izleyebilir. Çalışan veya iş ortağının bu politikada anlatılan ilkelere uymadığına dair bir kanıt olması halinde, Eko Global İsg iş akdinin sonlandırılması ve yasal yollar da dahil olmak üzere disiplin prosedürü uygulama hakkını saklı tutar.

13. Uygulama

Eko Global İsg tedarikçilerinin Bilgi Güvenliği Yönetim Sistemi çerçevesinde politika ve hizmet sunum kriterlerinin uygunluğunu gözden geçirme ve tetkik hakkına sahiptir.

Bu bilgi güvenliği politikasının ihlali Eko Global İsg'nin işlerinde zarara neden olur. Tedarikçinin herhangi bir çalışanı veya iş ortağının bu politikayı ihlali durumunda anlaşma/hizmet/sözleşme sonlandırmasına varan disiplin cezasına tabi olacaktır.

Onay:

Tedarikçi bu politikayı okuduğunu ve anladığını ve Eko Global İsg ile bir anlaşma/sözleşme kapsamında herhangi bir iş veya hizmete başlaması durumunda bu hüküm ve koşulları peşinen kabul etmiş olacağını beyan eder.

Hazırlayan	Onaylayan