QTERMINALS

BT (IT) GÜVENLİK POLİTİKASI

İçindekiler

1. AMAÇ VE POLİTİKA BEYANI

QTerminals, müşterileri, paydaşları ve Çalışanları adına tuttuğumuz bilgilerin öneminin bilincindedir. Buna göre, tüm bilgilerin güvenli, sorumlu ve emniyetli BT sistemleri ve uygulamaları aracılığıyla işlenmesi, saklanması, iletilmesi ve teslim edilmesi sırasında güvenliğini sağlamaya kararlıyız.

Bu BT Güvenliği Politikası (bundan böyle "Politika" olarak anılacaktır), BT güvenliği ve Şirket bilgilerinin korunması konusunda basit ve özlü bir şekilde genel rehberlik sağlamayı amaçlamaktadır. İlgili temel prosedürleri, rolleri ve sorumlulukları da özetleyen Bilgi Güvenliği Yönetim Sistemi (BGYS) Politika Kılavuzu'nda daha ayrıntılı rehberlik ve talimatlar sağlanmaktadır. Bu nedenle, hem Politika hem de BGYS Politika El Kitabı birbirinin yerine geçmediği veya birbirini geçersiz kılmadığı için tamamlayıcı olarak ele alınmalıdır.

2. UYGULAMA KAPSAMI

Politika küresel olarak tüm Çalışanlar için geçerlidir. Bu Politika herhangi bir ulusal veya uluslararası yasanın yerine geçmez. Herhangi bir çelişki durumunda mevzuat bu Politikaya göre öncelikli olmalıdır. Böyle bir çatışmanın tespit edilmesi durumunda çalışanların BT ekibini derhal bilgilendirmeleri rica olunur.

3. TANIMLAR

Çalışanlar, QTerminals'ın tüm çalışanları (sözleşmeli çalışanlar dahil), memurları ve yöneticileri anlamına gelir.

Etik İnceleme Paneli (ERP), QTerminals bünyesinde rapor edilen tüm etik dışı konular, suiistimaller ve suiistimalleri zamanında incelemeyi ve ilgili disiplin cezasına karar vermeyi taahhüt eden çok disiplinli bir organ anlamına gelir. ERP üyeleri, iddia edilen suiistimal ve/veya yanlış davranışın niteliğine ve ciddiyetine bağlı olarak Grup Hukuk ve Uyumluluk Direktörü tarafından vaka bazında seçilir.

Bölüm Yöneticisi, belirli bir Çalışanın doğrudan yönetim sorumluluğuna sahip olan kişidir.

QTerminals veya Şirket, QTerminals W.L.L anlamına gelir ve kontrol edilen bağlı ortaklıkları ve ortak girişimleri ifade eder.

4. BT GÜVENLİK YÖNERGELERİ

1. Şirket ekipmanlarına iyi bakın

Çalışanlar, görevlerini tamamlarken kullandıkları Şirket varlıklarından (örneğin yazıcılar) ve Şirket tarafından sağlanan kişisel ekipmanlardan (örneğin akıllı telefonlar, dizüstü bilgisayarlar) sorumludur. Şirketin ekipmanlarına iyi bakmak için Çalışanlar şunları yapmalıdır:

- Ekipmanı üreticinin spesifikasyonlarına göre çalıştırın ve bakımını yapın ve bu tür cihazların kaybolmaya, çalınmaya, hasara veya tahribata karşı korunmasına özen gösterin. İlgili Çalışanların ihmali veya kasıtlı suistimalinden kaynaklandığı değerlendirilen zararlardan çalışanlar sorumlu tutulacaktır.
- Ekipmanın arızalanması durumunda BT Yardım Masası ile iletişime geçin; BT Departmanı onarım işlemini gerçekleştirecektir.
- Çalışanların pozisyonuna veya ekipmanın ısmarlama konfigürasyonlarına göre tipik ekipmanın dışında bireysel ekipman almak için Bölüm Yöneticisinin ve BT Direktörünün onayını alın.

Şirketin ekipmanıyla ilgili olarak Çalışanların şunları yapması yasaktır:

- QTerminals'ın BT olanaklarını ve kaynaklarını, QTerminals dışındaki herhangi bir işletmenin operasyonları veya yönetimi ile bağlantılı olarak kullanmak.
- Ekipmanı başka bir Çalışana yeniden tahsis etmek. Ekipmanı tahsis etme ve yeniden tahsis etme yetkisi yalnızca BT Departmanına aittir.
- Şirket ekipmanına veya yazılımına müdahale etmek (örneğin, anti-virüs yazılımını devre dışı bırakmak veya değiştirmek).
- Masaüstü bilgisayarlar, yazıcılar, tarayıcılar gibi aygıtların QTerminals tesislerinden kaldırılması. İstisnai durumlarda bu cihazların kaldırılması Bilgi Güvenliği Sorumlusu, Veri Sahibi ve Yöneticinin yazılı özel onayını gerektirir. Bu, doğası gereği mobil olan cihazlar (dizüstü bilgisayarlar, tabletler ve akıllı telefonlar) için geçerli değildir ve bunlar Çalışanlar tarafından QTerminals tesislerine serbestçe taşınabilir.

Şirket varlıklarının korunmasına ilişkin daha fazla bilgiye ihtiyaç duymanız halinde lütfen BGYS Politika Kılavuzunun 10. Bölümüne bakınız. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım masasıyla iletişime geçin.

2. Tüm verileri sınıflandırın ve hassas verileri koruyun

Hassas verilerin korunması, ilk başta gizlilik, bütünlük ve kullanılabilirliğe dayalı olarak kritik değerlendirme ve sınıflandırma gerektiren çok adımlı bir süreçtir. Hassas verilerin korunmasını sağlamak için, Çalışanlar şunları yapmalıdır:

- Hassas bilgiler içeren tüm varlıkları, e-postaları, kayıtları ve medyayı Bilgi Sınıflandırma Politikasına göre "GİZLİ", "DAHİLİ" veya "KISITLI" sözcükleriyle işaretleyin. Açık bir görünürlük sağlamak için başlıklar, başlık sayfaları, pullar, etiketler vb. gibi göze çarpan yerlere ilgili işaretler konulmalıdır.
- Kamuya açık olmayan tüm bilgileri yetkisiz erişime ve gizlice dinlenmeye karşı koruyun.
- Kamuya açık olmayan tüm bilgileri kilitleyin ve Çalışanın masasında kimse bulunmadığında ekipmanı kilitleyin veya oturumu kapatın.
- Kısa bir süre işlem yapılmadığında tüm cihazları otomatik ekran kilitlemeye göre yapılandırın.
- Gizli bilgileri elektronik olarak iletmek için güvenli mesajlaşma (örn. şifrelemeli) kullanın (C3 sınıfı).
- Üçüncü bir tarafla hassas bilgi alışverişinde bulunmadan önce Gizlilik Anlaşmasının (NDA) imzalandığından emin olun.

Hassas verilerin korunmasıyla ilgili olarak, **Çalışanların şunları yapması yasaktır**:

- Birim Müdürü ve BT Direktörü tarafından onaylanmadığı sürece, taşınabilir depolama aygıtlarının (örneğin, kaybolmaya, çalınmaya, virüslere ve kötü amaçlı yazılımlara karşı savunmasız olmaları nedeniyle USB (evrensel seri veriyolu) bellekler, harici disk sürücüleri, SD kartlar) kullanılması.
- Diğer Çalışanların yerel sabit disklerinde saklanan dosyalara izinsiz olarak erişmek veya bunları görüntülemek de dahil olmak üzere, özel veya gizli olduğunu bildikleri veya bilmeleri gereken verilere erişmeye çalışmak.
- Birim Müdürü ve BT Direktörü tarafından onaylanmadıkça, Şirketle ilgili bilgileri depolamak veya paylaşmak için bulut hizmetlerini kullanmak.

Bilgi sınıflandırması hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BGYS Politika Kılavuzunun 9, 13 ve 14. Bölümlerine bakınız. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım masasıyla iletişime geçin.

3. İnternet ve İntranet'i dikkatli kullanın

İnternet, QTerminals Çalışanlarının günlük görevlerini tamamlaması için gerekli olmakla birlikte, kötüye kullanımı önemli riskler taşımaktadır. Bu nedenle Çalışanlar şunları yapmalıdır:

- İnternet faaliyetlerinin Şirketi olumsuz etkilememesini veya tartışmalı konularla ilişkilendirmemesini sağlayın. Bu kritik öneme sahiptir çünkü Çalışanın bilgisayarını tanımlayan bilgiler bir web sitesini ziyaret ederken kaydedilebilir. Bu nedenle, bir Çalışanın, QTerminals ağını kullanan herhangi bir yetkisiz ve/veya uygunsuz faaliyeti, QTerminals'ı ve itibarını etkileyebilir.
- QTerminals'ın BT Departmanı tarafından engellenen belirli web sitelerine ticari olarak erişmeye ihtiyaç duymanız durumunda yardım için BT Yardım masasıyla iletişime geçin.
- QTerminals'ın, bireylerin çalışma saatleri içerisinde internet bankacılığı veya çevrimiçi alışveriş gibi bazı kişisel görevleri yerine getirme ihtiyacını kabul ettiğini unutmayın. Ancak kişisel görevlerin iş sorumluluklarına göre öncelikli olmadığı ve QTerminals'ın üzerinde hiçbir şekilde olumsuz bir etkisi olmadığı varsayılarak buna izin verilir.

İnternet kullanımıyla ilgili olarak, Çalışanların şunları yapması yasaktır:
- Kurumsal İnternet veya İntranet'i aşırı derecede, kişisel kazanç için kullanmak.
- Diğer Çalışanların internet bağlantısını etkiliyorsa, büyük boyutlu kişisel dosyaları indirmek için kurumsal İnternet'i kullanmak.
- Uygunsuz içerik barındıran web sitelerini ziyaret etmek veya bu tür içerikleri indirmek. Uygunsuz içerik, siber suç, siber zorbalık veya pornografik içerik gibi yasa dışı ve uygunsuz kabul edilen her şeydir.
- Telif hakkıyla korunan herhangi bir materyalin lisans şartlarını ihlal edecek şekilde kullanılması veya indirilmesi (örn. korsan yazılım veya veriler).
- QTerminals'ın e-posta adresini kullanarak mesaj panolarını ve web günlüklerini (blogları) görüntülemek için kaydolmak veya yorum yapmak. Bu tür kaynaklara yalnızca salt okunur biçimde erişilebilir; erişim için etkileşimli oturum açmaya gerek yoktur.

İnternet ve İntranet'in bilinçli kullanımı hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BGYS Politika Kılavuzu Bölüm 16'ya bakınız. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım masasıyla iletişime geçin.

4. E-postaları profesyonel ve güvenli bir şekilde kullanın

E-postanın uygun şekilde kullanılmasını ve Şirket bilgilerinin korunmasını sağlamak için, Çalışanlar şunları yapmalıdır:
- E-postalarda profesyonel ve saygılı bir dil kullanın.
- Bu iletişim kanalı tamamen güvenli olmadığından ve içeriği iletim sırasında değiştirilebileceğinden, e-postanın meşru olup olmadığını değerlendirirken sağduyunuzu kullanın.
- Listenin uygun alıcıları içerdiğinden emin olmak için göndermeden önce e-postanın tüm alıcılarını doğrulayın.
- Şirketin e-posta sisteminde yapılandırılmış dağıtım listesini kullanırken dikkatli olun.
- E-postaları silerken dikkatli olun çünkü kurtarılmaları zordur. Eski e-postalar yedekleme sisteminde saklansa da bu, kurtarma amacıyla değil, arşivleme ve denetim amacıyla yapılır.
- Boyut sınırını aşan ekleri göndermek için QTerminals One Drive bağlantıları, büyük dosyaları sıkıştırmak veya daha küçük ekleri ayrı olarak göndermek gibi alternatif çözümler kullanın.
- Şirket tarafından sağlanan e-posta adresinin QTerminals'a ait olduğunu ve yalnızca iş yapma amacıyla sağlandığını unutmayın. Kişisel e-postaların ara sıra kullanılması, aşağıdaki koşullar sağlandığı sürece tolere edilebilir: (a) mesleki görevlerin yerine getirilmesine müdahale etmemesi, (b) iş sorumluluklarına göre öncelik vermemesi, (c) yersiz masraf veya yükümlülük doğurmaması, (d) QTerminals üzerinde hiçbir şekilde olumsuz bir etki yaratmaması.

E-postaların kullanımına ilişkin olarak, **Çalışanların şunları yapması yasaktır**:
- Kötü ve/veya müstehcen dil kullanmanın yanı sıra yanıltıcı içerik, spam veya zincirleme e-postalar kullanmak.
- Kişisel e-postayı iş amacıyla kullanmak.
- QTerminals Çalışanları arasındaki dahili e-postalar için "KKK" fonksiyonunun kullanılması.

- Harici e-postaların doğasında bulunan güvenlik riskleri nedeniyle şüpheli e-posta adreslerinden alınan, şüpheli içerik içeren veya tanınmayan kişi veya kuruluşlardan alınan içeriklere sahip e-postaların açılması. Bu e-postaların ek içermesi durumunda bunları açmayın. Bunun yerine, daha fazla tavsiye için BT Yardım Masasını bilgilendirin.
- Halka açık web sitelerini çevrimiçi alışveriş gibi ticari olmayan amaçlarla kullanırken QTerminal e-posta adresinin sağlanması.
- Başka bir Çalışanın e-postalarını izinsiz okumak. Yöneticinin asistanına takvim erişim haklarını sağlaması bir istisnadır ve yöneticinin açık yetkilendirmesini gerektirir.
- İstense bile müşterilerin, satıcıların, paydaşların e-postalarını kişisel e-postalarına (örn. Gmail) göndermek.

E-posta güvenliği hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BGYS Politika Kılavuzunun 17. Bölümüne bakın. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım masasıyla iletişime geçin.

5. BT güvenlik tehditlerine karşı dikkatli olun

Kötü amaçlı yazılım, sosyal mühendislik ve lisanssız yazılım kullanımı, BT güvenlik sistemlerine yönelik en önemli tehditler arasındadır. QTerminals verilerine yetkisiz erişim riskini önlemek için, **Çalışanlar şunları yapmalıdır:**

- Şirketin ekipmanlarında yalnızca lisanslı ve onaylanmış yazılımları kullanın.
- USB sabit diskler, ağ dosyaları, e-posta ekleri ve İnternetten dosyalar da dahil olmak üzere herhangi bir kaynaktan indirilen dosyaları kullanmadan önce virüs taraması yapın.
- Bazı bilgisayar korsanları tarafından Şirket içindeki kritik bilgilere erişim sağlamak için kullanılan sosyal mühendislik ve psikolojik manipülasyonlara karşı dikkatli olun (örneğin yalan vaat olarak da bilinen kandırma yoluyla).
- Standart dışı herhangi bir yazılımın (örn. AutoCAD, Bloomberg) kurulumu için Bölüm Müdürü ve BT Direktöründen onay alın.

BT güvenlik tehditleriyle ilgili olarak, **Çalışanların şunları yapması yasaktır**:

- QTerminals BT sistemi ile ilgili şifreler gibi hassas bilgilerin yazılı veya sözlü olarak Şirket dışından herhangi biriyle paylaşılması.
- Yetkisiz yazılım programlarının indirilmesi, kurulması veya kullanılması. Bilgisayarların uzaktan kontrol edilmesine izin veren yazılımların yanı sıra paket dinleme, parola tespit etme ve diğer bilgisayar korsanlığı araçları açıkça yasaktır.
- Kaynağı bilinmeyen programların yürütülmesi.
- QTerminals BT kaynaklarını kullanarak QTerminals sistemlerine veya herhangi bir harici sisteme karşı herhangi bir bilgisayar korsanlığı faaliyeti yürütmek.
- Bilinçli olarak tanıtmak:
  - her türlü bilgisayar virüsü, solucan, truva atı veya tuzak kapısı program kodu.
  - herhangi bir bilgisayarı, sunucuyu veya ağ bileşenini aşırı yüklemek, bunları devre dışı bırakmak veya hizmet reddi gibi saldırılar oluşturmak üzere tasarlanmış cihazlar veya programlar.
  - Çalışanların ve verilerin gizliliğini veya güvenliğini korumayı amaçlayan herhangi bir sistemi atlatmak için tasarlanmış herhangi bir cihaz veya program.

Yazılım kurulumu hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BGYS Politika Kılavuzunun 18, 20 ve 27. Bölümlerine bakınız. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım masasıyla iletişime geçin.

6. Güvenli şifreler seçin

İhmal edildiğinde parolalar BT güvenlik sisteminin savunmasız bir unsuru haline gelebilir. Şirket verilerine yetkisiz erişim riskini azaltmak için, **Çalışanlar şunları yapmalıdır:**

- İlk kez oturum açtıktan sonra şifreyi hemen değiştirin.
- Şifrenizi düzenli olarak değiştirin (en az 42 günde bir).

- En az 8 karakter ve en az 1 özel karakter, rakam, büyük ve küçük harflerden oluşan şifreyi seçiniz.
- Başka hiçbir yerde kullanılmayan QTerminals cihazları için özel bir şifre seçin (örn. kişisel e-posta, sosyal medya hesapları vb. için).

Şifrelerle ilgili olarak, **Çalışanların şunları yapması yasaktır**:

- Yetkili QTerminals BT ekibi dışında herhangi birine şifreyi açıklamak (teknik destek amacıyla). BT ekibine açıklanması durumunda parola, BT sorunu çözüldükten hemen sonra değiştirilmelidir.
- BT ekibi tarafından özel olarak izin verilmedikçe genel veya paylaşılan parolaların kullanılması.
- Şifreleri düz metin olarak (şifrelenmemiş) yazmak.

Şifre politikası hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BGYS Politika Kılavuzu Bölüm 25'e bakınız. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım ofisiyle iletişime geçin.

7. Onaylanmış mesajlaşma ve video konferans araçlarını kullanın

Çalışanlar mesajlaşma ve video konferans için Microsoft Teams **kullanmalıdır**. Microsoft Teams her masaüstü ve dizüstü bilgisayara dağıtılır ve iş biriminizdeki Çalışanlarınızın cep telefonlarına dağıtılabilir.

Mesajlaşmayla ilgili olarak, **Çalışanların şunları yapması yasaktır**:

- İçerdiği güvenlik riskleri nedeniyle işle ilgili bilgi veya belge alışverişinde bulunmak için sosyal ağları veya WhatsApp gibi kişisel anlık mesajlaşma yazılımlarını kullanmak.
- Bir sosyal ağa kaydolmak veya QTerminals ve işleri hakkında herhangi bir bilgi yayınlamak için QTerminals e-postasını kullanmak. Kurumsal İletişim Departmanı, QTerminals'ın sosyal ağlardaki varlığını yönetmekten sorumlu tek departmandır.

QTerminals'ta mesajlaşmanın kullanımı hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BT Yardım ofisine ulaşın.

8. Evden çalışırken Şirketin bilgilerini koruyun

BT Departmanı, işi kolaylaştırmak için Çalışanlara, rol görevlerinin gerektirdiği şekilde, QTerminals BT sistemlerine uzaktan erişime izin veren VPN (sanal özel ağı) hesapları verebilir. Çalışanlar, QTerminals ağına kişisel bir bilgisayardan erişirken, yetkili olmayan herhangi bir kişinin herhangi bir QTerminals BT sistemine veya verilerine erişimini engellemelidir.

Evden çalışmayla ilgili olarak, **Çalışanların şunları yapması yasaktır**:

- VPN bağlantısı olmadan genel Wi-Fi ağlarını kullanma.
- QTerminals BT sistemlerine genel bilgisayarlardan erişim.
- Kişisel VPN hesap ayrıntılarının başka bir Çalışana veya üçüncü tarafa iletilmesi.
- Herhangi bir kamu bilgisayarında materyallerin basılması.

Evden çalışma politikası hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen iş biriminizin BT Yardım ofisi ile iletişime geçin.

9. Kişisel cihazları kullanmadan önce onay alın

Kişisel cihazları işle ilgili amaçlarla kullanmak için, **Çalışanlar şunları yapmalıdır**:

- Yalnızca Çalışanların sahip olduğu mobil cihazların veya tabletlerin yapılandırılabileceğini ve QTerminals e-posta sistemine ve Microsoft Teams işbirliği aracına bağlanabileceğini unutmayın. Doğrudan Çalışan tarafından satın alınan diğer ekipmanlar, güvenlik riskleri nedeniyle QTerminals BT sistemlerine yapılandırılamaz veya bağlanamaz.

- BT ekibinden onay ve yapılandırma desteği isteyin.
- Şirketin kaynaklarına erişmek için kişisel dizüstü bilgisayar, akıllı telefon veya tableti kullanmadan önce ilgili QTerminals politikalarını okuyun ve imzalayın.

Kişisel cihazların kullanımına ilişkin daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BGYS Politika Kılavuzu Bölüm 22'ye bakınız. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım ofisile iletişime geçin.

10. Bir güvenlik açığı fark ederseniz BT ekibiyle iletişime geçin

Çalışanlar, aşağıdakilerden herhangi birinin gözlemlenmesi durumunda derhal BT ekibine rapor vererek QTerminals BT sisteminin güvenli olmasını proaktif bir şekilde **sağlamalıdır**:

- Verilere yetkisiz erişim veya değişiklik.
- Kötü amaçlı yazılımlar/virüsler.
- BT kaynaklarının uygunsuz kullanımı.
- Şüpheli veya olağandışı faaliyetler.
- QTerminals'in BT güvenliğini tehlikeye atan diğer zayıflıklar.

Olay yönetimi hakkında daha fazla bilgiye ihtiyaç duymanız durumunda lütfen BGYS Politika Kılavuzunun 33. Bölümüne bakın. BGYS Politika Kılavuzu sorunuza yanıt vermiyorsa lütfen iş biriminizin BT Yardım ofisile iletişime geçin.

5. ÇALIŞAN VERİLERİNE ERİŞİM

QTerminals, BT sistemlerinde (kişisel bilgisayarlar, dizüstü bilgisayarlar, tabletler ve akıllı telefonlar dahil) bulunan verilerden nihai olarak sorumludur. QTerminals ayrıca veri korumayla ilgili geçerli mevzuata uymayı da taahhüt eder. Buna göre QTerminals, Çalışanın verilerine ve iletişimlerine aşağıdaki nedenlerden dolayı erişebilir:

- Polis soruşturmaları için kanıt sağlamak.
- Kanun ve düzenlemelere uyulmasını sağlamak.
- QTerminals'ın iç prosedürlerine, politikalarına ve sözleşmelerine uyulmasını sağlamak.
- Yasal ve düzenleyici yükümlülüklere uymak.
- QTerminals sistemlerinin yasa dışı faaliyetlerini veya yetkisiz kullanımını araştırmak ve önlemek.

Şirketin BT güvenliğini sağlamak amacıyla BT Departmanı, Çalışanlarla ilgili aşağıdaki verilere onların önceden izni olmadan erişebilir ve bunları izleyebilir:

- Virüs/istenmeyen posta önleme yazılımı tarafından engellenen potansiyel olarak zararlı e-postalar (istenmeyen pazarlama e-postaları (spam) ve anormal eklere sahip e-postalar dahil). Bu tür e-postaların virüs içermesi durumunda işlenmesi ve silinmesi için Bilgi İşlem Departmanının erişime ihtiyacı vardır.
- İnternet trafiği verileri ve gezinme (etki alanı adları, ziyaret edilen web siteleri, ziyaretlerin süresi, internetten indirilen iş dışı dosyalar ve boyutları dahil). Herhangi bir anormal gezinme veya ihlal, daha fazla önlem alınması için BT Direktörüne rapor edilecektir.
- Merkezi sistemlere, (ERP, TOS vb. gibi) günlüklere erişim. Herhangi bir anormal davranış BT Direktörüne rapor edilir.
- VPN erişim oturumu açmak. Herhangi bir anormal davranış BT Direktörüne rapor edilir.

Bilgi İşlem Departmanı, Çalışanın rızası alınmadıkça veya bir polis soruşturması söz konusu olmadığı sürece Çalışanların diğer iletişimlerini veya verilerini izlemez. Ancak bu genel kural aşağıdaki durumlarda geçerli olmayabilir:

- Çalışanın yokluğu (hastalık, izin, ölüm veya başka bir nedenden dolayı) ve müsait olmaması durumunda, QTerminals Grup Çeşitlilik Direktörü, Grup BT Direktörü ve Grup Hukuk ve Uyumluluk Direktörünün talimatı üzerine makul araçları (telefon gibi) kullanarak.
- Grup Hukuk ve Uyum Direktörünün onayı ile QTerminals varlıkları kullanılarak yasa dışı faaliyetlerin yürütüldüğüne dair ciddi şüphelerin olması durumunda.
- Çalışanın iş ve operasyonların devamlılığı amacıyla Şirketten ayrılması durumunda. Özel mesajları ve verileri gizli tutarken, görevini devralan Çalışana ilgili e-postalara ve belgelere erişim sağlanabilir.

6. SORUMLULUKLAR

Tüm Çalışanlar bu Politikaya uymaktan sorumludur. Çalışanların bu Politikanın ve BGYS Politika Kılavuzu da dahil olmak üzere QTerminals tarafından yayınlanan ek politika ve prosedürlerin tüm yönlerini okumasını, anlamasını, kabul etmesini ve bunlara uymasını bekliyoruz. Tüm Çalışanların, sorularını açıklığa kavuşturmak, bilgi talep etmek veya endişelerini ifade etmek için kendi iş birimlerindeki BT Yardım masasıyla iletişime geçmesi teşvik edilir. Bölüm Yöneticileri, BT departmanının ilgili rehberliğiyle birlikte, Çalışanların BT güvenliğiyle ilgili endişelerinin giderilmesini sağlayacaktır.

Yönetim, bu Politikanın uygulanması için gerekli araçların, kaynakların ve personelin mevcut olmasını sağlamaktan sorumludur. QTerminals'ın liman veya terminal seviyesindeki her yönetici üst düzey yöneticisi, sorumlu oldukları iş biriminin bu Politikaya tamamen uygun olmasını ve bu Politikaya ilişkin farkındalığı ve anlayışı teşvik ederek ve bu Politikanın etkili bir şekilde uygulanması için yeterli kaynakların tahsisini sağlayarak bu Politikaya tam olarak uymasını sağlamalıdır. BT ekibi özellikle bu Politikaya uyulmasını sağlayacak gerekli süreçlerin mevcut olduğundan emin olmalıdır.

7. KONUŞUN

QTerminals, Çalışanlarının bu Politikanın herhangi bir ihlalini veya ihlal şüphesini QTerminals veya üçüncü taraflardan herhangi birine bildirmeye teşvik edildiği bir dürüstlük ve şeffaflık ortamını destekler. Raporlama ya Birim Yöneticilerini, İK departmanlarını, Uyum Görevlisini/Temsilcisini bilgilendirerek ya da alternatif olarak QTerminals intranetinde, QTerminals web sitesinde ve özel bir telefon hattında bulunan QTerminals Etik Hattı aracılığıyla yapılacaktır.

Ayrıca, Politikanın bilinen veya şüphelenilen bir ihlalini fark eden ve bildiren kişilere karşı herhangi bir misilleme yapılması kesinlikle yasaktır. İyi niyetle bir ihlali bildiren bir kişiye karşı misilleme yaptığı kanıtlanan herkes, disiplin cezasına tabi tutulacaktır. Ancak, herhangi bir yanlış veya kötü niyetli iddia, iş akdinin feshine kadar varabilecek uygun disiplin ve yasal işlemlere yol açabilir.

İhbar süreci hakkında daha fazla bilgi için lütfen **QTerminals İhbar ve Dolandırıcılıkla Mücadele Prosedürlerine** bakın.

8. DİSİPLIN CEZASI

QTerminals'ta, "Uygulama Kapsamı"nda belirtildiği üzere, bu Politikanın geçerli olduğu herkesin bu Politikaya uyması beklenmektedir. Bunların herhangi bir şekilde ihlali disiplin cezası, iş akdinin feshi veya yasal işlemlerle sonuçlanabilir.

Yanlış davranışlara ilişkin şikayetlerin soruşturma gerektirmesi durumunda, sonuçları ve önerilen düzeltici eylemler Etik İnceleme Paneli (EİP) tarafından incelenecek soruşturmalar yapılacaktır. Düzeltici eylemler, davranış ihlaline ilişkin gerçekler ve koşullar ile soruşturmanın sonuçlarına göre belirlenecektir.

İddia edilen suiistimal ve Davranış Kuralları veya bu Politikanın ihlaline ilişkin soruşturma süreci hakkında daha fazla bilgi için lütfen **QTerminals İhbar ve Dolandırıcılıkla Mücadele Prosedürlerine** bakın.

9. İNCELEME SÜRECİ

BT ekibi bu Politikanın yeterliliğini ve etkinliğini periyodik olarak değerlendirecektir. Bu incelemelerin sonuçlarına bağlı olarak değişiklik önerilebilir ve sunulabilir.

Belgeyi onaylayan:

Grup İcra Kurulu Başkanı
Neville Bissett