İş ve BT Sürekliliği Planı

GEDİK YATIRIM MENKUL DEĞERLER A. Ş

BELGE TARİHÇESİ

YÜRÜRLÜK TARİHİ	BELGE NO	GÜNCELLEME NO	AÇIKLAMA	HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN
25.09.2019	PLN-BGYS-1	1	SPK Bilgi Sistemleri Yönetimi Tebliği (VII-128.9)	BİLGİ GÜVENLİĞİ SORUMLUSU	İÇ KONTROL SORUMLUSU	YÖNETİM KURULU

İÇİNDEKİLER

1. GİRİŞ

İş ve BT Sürekliliği Planları; Kurum'un faaliyetlerini etkileyen bir kesinti ya da olağanüstü bir durum yaşanması sonrasında, kritik iş birimlerinin ve aktivitelerin sürekliliğini sağlamak amacıyla hazırlanmış kurtarma stratejilerini ve aksiyonlarını kapsamaktadır. Kurtarma stratejileri ve aksiyonlar Kurum hizmetleri baz alınarak oluşturulmuştur. İş ve BT Sürekliliği Planları olmayan kurumların, kritik süreçlerinde/aktivitelerinde yaşayacakları kesintiler sonucu itibar/saygınlık kaybı (imaj) yaşamma, finansal zarara uğrama, uyum açısından zor duruma düşme ve kendisine bağımlılığı olan üçüncü tarafları kötü yönde etkileme ihtimalleri daha yüksektir.

İş Sürekliliği Planları'nın, Yönetim Kurulu'nun yetki verdiği Bilgi Güvenliği Yöneticisi tarafından yürütülmesi sağlanır. İş Sürekliliği Planları; İş Sürekliliği Planı, BT Süreklilik Planı ve eklerinden oluşmaktadır. Plan dahilinde görevli personelin hem İş Sürekliliği Planı'na hem de kendisi ile ilgili kurtarma planlarına (varsa ilgili ek dokümanlara) hakim olması gerekir.

2. AMAÇ VE KAPSAM

İş Sürekliliği Planları; Kurum çalışanları, müşterileri ve Kurum kaynakları (teknoloji, ekipman) için güvenli bir çevre oluşturmak, olağanüstü durumlar için hazırlıklı olmak, olay anında ve sonrasında yapılacak işlemleri tanımlamak, Kurum süreçlerine/aktivitelerine minimum kesinti ve zararla devam etmesini sağlamak amacıyla hazırlanmıştır.

Doküman dahilinde; türü ve sebebi ne olursa olsun, herhangi bir kesinti ya da olağanüstü durumda, Kurum'un kritik iş süreçlerinin/aktivitelerinin sürekliliğini sağlayan iş sürekliliği planlamasının alt başlıkları ifade edilmiştir.

İLGİLİ TEBLİĞ	
Tebliğ	**Alt Maddeleri**
SPK Bilgi Sistemleri Yönetimi Tebliği	Madde 7 – Üst yönetimin gözetimi ve sorumluluğu 7/6: Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanır. Planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı belirlenir. Madde 26 – Bilgi sistemleri sürekliliği 26/2: Kurum, Kuruluş ve Ortaklıklar faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planını hazırlar. 26/3: Plan kapsamında ikincil sistem tesis edilir ya da bu hizmeti destek hizmeti kuruluşlarından tedarik etme hususunda güvence sağlayan anlaşmalar yapılır. İkincil sistemde, Kurum, Kuruluş ve Ortaklıkların veri ve sistem yedekleri kullanıma hazır bulundurulur. 26/4: Plan, iş süreklilik planında belirlenen hedefleri de dikkate alacak şekilde, kritik iş süreçlerini destekleyen bilgi sistemleri hizmetlerine yönelik hazırlanır. Bu çerçevede hizmetlerin tekrar kullanıma açılmasını sağlayacak alternatifli kurtarma süreç ve prosedürleri tesis edilir ve gerekli önlemler alınır. 26/5: Plan kapsamında, performans takibi ve kapasite planlaması yapılır, sistem kaynaklarının kullanımı izlenir. 26/6: Bilgi sistemleri altyapısından kaynaklanabilecek kesintilere, işlem performansını düşürecek veya iş sürekliliğini aksatacak durumlara karşı gerekli önlemler alınır. 26/7: Bilgi sistemlerinin sürekliliğini sağlamak amacıyla, risk değerlendirmesi, risk azaltma ve risk izleme faaliyetleri gerçekleştirilir.

	26/8: Plan, iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra gözden geçirilerek güncellenir. Planın etkinliğini ve güncelliğini temin etmek üzere testler yapılır, testlere varsa dış kaynak yoluyla hizmet alınan kuruluşlar da dâhil edilir ve test sonuçları üst yönetime raporlanır. Testler, her yıl tekrarlanır. 26/9: Bilgi sistemleri, iş sürekliliği planındaki önceliklere uygun olarak yedeklenir ve yedekten geri dönülmesi için gerekli süreçler bilgi sistemleri sürekliliği planına ve testine dâhil edilir. 26/10: Kurum, Kuruluş ve Ortaklıklar, bilgi güvenliği politikasının, bilgi sistemleri süreklilik planının, ağ topolojisinin, bilgi sistemleri varlık envanteri ile iş sürekliliği ve güvenliği açısından önem arz eden diğer dokümanların güncel sürümlerini ve bilgi sistemleri yönetimine ilişkin parolalarını güvenli ortamlarda saklar.

3. TANIMLAR ve KISALTMALAR

Kurum: Gedik Yatırım Menkul Değerler A. Ş

Yönetim Ekibi: Üst Yönetim

Kurtarma Zamanı Hedefi (RTO): Kurumsal BT Hizmetinin yeniden verilmeye başlanma ya da Kaynakların kurtarılma süresi.

Kurtarma Noktası Hedefi (RPO): Kurumsal BT Hizmetini kaldığı yerden başlatmak için işlemi etkinleştirmesi amacıyla, bir hizmette kullanılan bilginin tekrar dönülmesi gereken nokta.

Olağanüstü Durum Merkezi (DRC): Kurumsal BT Hizmetinin kesintisiz çalışması ve Kurum verilerinin bütünlük ve erişebilirliğinin sürdürülmesi amacıyla tüm Kurum verilerinin tutulduğu farklı bir konum.

İş Sürekliliği Merkezi (İSM): İş Sürekliliğinin sağlanması amacıyla, Kurum bünyesinde Avrupa yakası Şişli yerleşiğinde Şişli Şube İş Sürekliliği merkezi, alternatif acil ve olağanüstü durumlar için merkez dışı (re-lokasyon) örgüt olarak tespit edilmiştir.

İş Etki ve Risk Analizi: İş süreçlerinin ve bir faaliyet kesintisinin iş süreçleri üzerinde oluşturabileceği etkilerin analiz süreci.

Bilgi Sistemleri Sürekliliği: Faaliyetlerin sürdürülmesini sağlayan bilgi sistemleri servislerinin bir kesinti durumunda sürekliliğinin sağlanmasına yönelik hazırlanan ve iş sürekliliği planının bir parçası olan plan.

İş Sürekliliği Planı: İş sürekliliği yönetiminin bir parçası olan ve bir kesinti durumunda Kurum'un öncelikleriyle uyumlu olarak faaliyetlerin sürdürülmesine ve mevzuata uyum sağlanmasına yönelik politika, standart ve prosedürlerden oluşan yazılı planlar bütününü.

4. HEDEF VE VARSAYIMLAR

İş Sürekliliği Planları'nın temel hedefi bir kesinti ya da olağanüstü durum sonrasında Kurum'un kritik süreçlerini/aktivitelerini belirlenmiş kabul edilebilir süreler içerisinde aktif hale getirmektir. Diğer hedefler aşağıdaki gibi detaylandırılabilir:

- Kurum çalışanlarını ve müşterilerini korumak, sağlık ve refahından emin olmak,
- Kurum varlıklarının korunmasını sağlamak, zararı en aza indirmek,
- Olağanüstü durumun yarattığı tehditleri kontrol etmek, gerekli önlemleri almak,
- Olayın büyüklüğünü değerlendirmek, karşılaşılan zararı en aza indirmek,
- Yasal yükümlülüklerin her an ve her zaman yerine getirilmesini sağlamak,
- Kurum'un marka imajını ve saygınlığını korumak,

- Acil ve olağanüstü durum sırasında hataların oluşmasını önleyici prosedürleri devreye almak, uygulamak ve iş yapış şekillerindeki hataları önlemek,
- Kritik faaliyetleri belirlenen süreler içerisinde başlatmak ve iletişimi yönetmek,
- Acil ve olağanüstü durum sonrasında ortaya çıkan sorunları ve sonuçları değerlendirmektir.

Kurum, İş Etki ve Risk Analizi çalışmasını da değerlendirerek aşağıdaki senaryolar için planın oluşturulmasına karar verilmiştir.

- Binaların kullanımına engel teşkil eden bir durumun yaşanması
- Bilgi sistemleri kesintisi
- Kritik personele ulaşılamaması

İş Sürekliliği Planı kapsamında dikkate alınan varsayımlar aşağıdaki gibidir:

- Alternatif lokasyonlar ve lokasyonların altyapı sistemleri kullanılabilir durumdadır.
- Çalıştırılacak uygulama ve işletilecek süreçler/aktiviteler için kabul edilebilir kesinti süreleri ve veri kurtarma noktası hedefleri, analiz sırasında belirlenen değerler (RTO/RPO) ile uyumlu haldedir.
- BT bileşenleri için gerekli veri kurtarma noktası hedeflerine (RPO) uygun yedekleme mekanizmaları kurulmuş ve test edilmiş durumdadır.
- Uzaktan çalışma talimatları, gerekli donanımlar, donanım üzeirndeki uygulamalar (laptop, VPN, telefon), hesaplar hazır durumdadır.
- Acil ve olağanüstü durumda görev alacak ekiplerin hem kendi hem ekip üyelerinin hem de diğer ekiplerdeki üyelerin erişim bilgileri mevcuttur. Kullanılabilen tüm iletişim araçları ile haberleşme sağlanır.
- Süreçlerin/aktivitelerin gerçekleştirilmesi için bağımlı olunan kurum ve kuruluşlar ile iletişim kurulabilir durumdadır, kontak kişilerin erişim bilgileri mevcuttur.
- Acil ve olağanüstü durumda çalışacak minimum personel sayısı ve hangi personelin çalışacağı belirlenmiş durumdadır. Bu personel, acil ve olağanüstü durumda nasıl davranacakları, kimlerle bağlantıya geçecekleri ve işlerini nasıl devam ettirecekleri konusunda bilgi sahibidir.
- Olağanüstü durum süresince ortaya çıkacak ek masrafları onaylamak üzere bir ya da birden fazla Üst Yönetici (Yönetim Ekibi) hazır bulunur.

5. İŞ SÜREKLİLİĞİ PLANININ BAŞLATILMASI

Kurum, kontrol dışı/beklenmedik ve hizmet kesintileri yaratabilecek olaylar için senaryolar oluşturmuş, bu tür durumlarda alınacak aksiyonları belirlemiştir. Yaşanan kesintinin 12 saat içerisinde geri kazanılamayacağının tespit edilmesi durumda CEO tarafından olağanüstü durum ilan edilerek İş Sürekliliği Planı devreye alınır. Karar süreci, eğer acil ve olağanüstü durum çalışma saatleri içerisinde gerçekleştiyse durumun saptanmasından itibaren 2 (iki) saat içerisinde, çalışma saatleri dışında gerçekleştiyse 4 (dört) saat içerisinde tamamlanır. CEO'nun vereceği karara istinaden durumun kritikliğine göre iş süreçlerinin tamamının ya da sadece kritik olanların çalışmasına karar verilebilir. Olağanüstü durum 'un ilanı sonrasında personel ve yönetim kadrosuna gerekli bilgilendirmeler yapılır. Belirlenen sayıda personel karar verilen alternatif çalışma sahasına gider ya da çalışmalarına evden devam eder. İş Kurtarma Ekipleri görevli oldukları kritik iş süreçleri için hazırlanan kurtarma planlarını uygular ve mevcut durumu düzenli olarak raporlar. Acil Durum Ekipleri ise olaya müdahele eder.

6. TOPLANMA MERKEZİ

Mesai saatleri içerisinde meydana gelen bir olağanüstü durum veya kesintide Yönetim Kurulu Kurum'da toplanır. Binanın kullanılamaz durumda olması halinde üyeler cep telefonları aracılığıyla birbirleri ile iletişim kurarlar. İlk değerlendirmenin ardından üyeler hasar görmemiş İSM lokasyonunda toplanırlar, fiziksel olarak toplanmaya gerek görülmezse telekonferans

yoluyla (mümkünse) bir araya gelirler. Binanın hasar görmesi durumunda kurum toplanma merkezinde toplanılır.

Mesai saatleri dışında meydana gelen bir olağanüstü durum ya da kesintide, cep telefonları ile Yönetim Kurulu ve Bilgi Güvenliği Yöneticisi birbiriyle iletişim kurar. İlk değerlendirmenin ardından üyeler hasar görmemiş İSM lokasyonunda toplanırlar, fiziksel olarak toplanmaya gerek görülmezse telekonferans yoluyla (mümkünse) bir araya gelirler.

7. PERSONEL YÖNETİMİ

Olağanüstü durum sonrası alınan kararlar doğrultusunda personel ve yönetim kadrosuna gerekli bilgilendirmeler Bilgi Güvenliği Yöneticisi tarafından yapılır. Ana ilke, herkesin bilmesi gerektiği kadar bilgilendirilmesidir. İş Kurtarma Ekipleri, Bilgi Güvenliği Yöneticisi koordinasyonunda, karar verilen alternatif çalışma sahasına gider.

8. ACİL DURUM SENARYOLARI

7.1. Yangın

Yangını çağrıştıracak bir durum ile karşılaşıldığında (duman, yanık kokusu, vb.) ya da doğrudan yangın tespit edildiğinde (otomatik/manuel) tüm personelin yapması gerekenler aşağıda belirtilmiştir:

- Duman detektörlerinin yangını algılamadığı durumlarda personel tarafından yangın ihbar butonları kullanılır. Yangın ihbar butonları, ortamda yangın belirtilerinin fark edilmesi halinde manuel olarak yangın alarmı vermeyi sağlar.
- Çalışanlar, Acil Durum Ekibi'nin talimatları doğrultusunda çalışma ortamındaki gerekli güvenlik önlemlerini alarak bulunduğu alanı hızlı ve dikkatli bir şekilde terk eder ve Kurum'un belirlenen yerindeki toplanma alanına gider.
- Tehlike çıkış merdivenleri kargaşaya sebebiyet vermeden kullanılır. Kesinlikle asansör kullanılmaz.
- Görgü tanıkları veya bina güvenliği tarafından ilgili yerlere (itfaiye, cankurtaran, polis, vb.) bilgi verilir.

7.2. Deprem

Sarsıntı başladığında personel tarafından yapılması gerekenler aşağıda belirtilmiştir:

- Personel; dolap gibi devrildiğinde yaralayıcı olabilecek eşyalardan uzak durarak, başını çanta, minder, kitap, klasör gibi eşyalarla koruyarak kendine güvenli bir yer bulur. Burası kolon, perde duvarlarının yanı ya da masa altları olabilir. Masanın altına girilip baş iki el ile örtülerek cenin pozisyonunda üzerine düşen eşyalardan korunur.
- Çalışanlar, Acil Durum Ekibi'nin talimatları doğrultusunda çalışma ortamındaki gerekli güvenlik önlemlerini alarak bulunduğu alanı hızlı ve dikkatli bir şekilde terk eder ve Kurum belirlenen merkezdeki yerindeki toplanma alanına gider.
- Tehlike çıkış merdivenleri kargaşaya sebebiyet vermeden kullanılır. Kesinlikle asansör kullanılmaz.
- Görgü tanıkları veya bina güvenliği tarafından ilgili yerlere (itfaiye, cankurtaran, polis, vb.) bilgi verilir.

7.3. Terörizm

Terörist saldırısının (savaş vb.) söz konusu olduğu durumlarda yapılması gerekenler aşağıda belirtilmiştir:

- Görgü tanıkları veya bina güvenliği tarafından ilgili yerlere (itfaiye, cankurtaran, polis, vb.) bilgi verilir.
- Binanın tahliyesine polis ile beraber karar verilir, binadan tahliye olan personel toplanma yerine gider.
- Acil Durum Ekibi olaya müdahele eder.

9. Bilgi Teknolojileri Süreklilik Planı

8.1. İş Kurtarma Stratejileri

İş kurtarma stratejileri aşağıdaki gibidir:

- Öncelikli süreçlerin ve sistemlerin tespiti için tüm iş birimleri ile yapılan iş etki analizlerinin sonucunda belirlenen Kurtarma Zamanı Hedefi (RTO) ve Kurtarma Noktası Hedefi (RPO) kullanılır. Sistem Odası, Olağanüstü Durum Merkezi (DRC) ve içerisindeki sistemler bu doğrultuda olağanüstü duruma hazırlanır. Ayrıca kıymetli evraklar ve sürecin devamlılığı/yedekliliği için saklanması gerekli olan yazılı/basılı dokümanlar da bu doğrultuda gözden geçirilir.
- Kurtarma Zamanı Hedefi ve Kurtarma Noktası Hedefi 5 ayrı zaman dilimine yayılır:
- 0-6 saat,
- 6 saat-12 saat,
- 12 saat-24 saat,
- 24 saat-48 saat,
- 48 saat üstü.
- Bir gün içerisinde kurtarılması hedeflenen aktiviteler yüksek öncelikli olarak değerlendirilmektedir. Yüksek öncelikli aktivitelerin kurtarılmasına önem verilir.
- Veri kurtarma hedefi 12 saate kadar olan sistemler Yüksek Öncelikli olarak değerlendirilmektedir. Yüksek öncelikli olarak belirlenen sistemlerin kurtarılmasına önem verilir.
- İş kurtarma faaliyetleri temel olarak aşağıdaki 2 yöntemden birisi ile yapılır:
  - İşlemlerin manuel olarak devam ettirilmesi (çalışma alanından bağımsız olarak)
  - Sistem Odası'nda bulunan yedek sistemler veya Olağanüstü Durum Merkezi'nde bulunan sistemler aracılığıyla faaliyetlerin devam ettirilmesi
- İdari Birimler bina bağımsız çalışabildiği için ilk aşamada, İSM lokasyonunda Kurum tarafından tahsis edilmiş dizüstü bilgisayarlara kurulu VPN bağlantısı ile çalışılır.
- Uygulamalara uzaktan bağlantı hakkı verilebilecek personel (çalışmalarını bireysel olarak devam ettirebilecek) belirlenir, gerekli bilgilendirmeler yapılır, ilgili altyapı ve kaynaklar hazırlanır.
- Olağanüstü durum 'da çalışmak üzere minimum personel sayısı, personel bilgileri ve yedekleri önceden belirlenir. Bu personele olağanüstü durumda nasıl davranacakları, kimlerle bağlantıya geçecekleri ve işlerini nasıl devam ettirecekleri konusunda bilgi verilir.
- Çalışan kişiler ve yönetim kadrosuna mevcut duruma ve alınan kararlara ilişkin bilgilendirme (iletişimin tahsisi) İletişim Ekibi tarafından gerçekleştirilir. Alternatif çalışma sahasına ulaşımı İnsan Kaynakları Birimi koordine eder.
- Medya ile iletişimi, mevcut durum ile ilgili kamu ve özel kurum bilgilendirmelerini İletişim Ekibi gerçekleştirir.
- İş kurtarma faaliyetleri, planlarda yazıldığı gibi belirlenen personel tarafından yerine getirilir. BT Birimi son kullanıcı desteği, saha gözetimi ve koordinasyonun sağlanması konularında görevlidir.
- BT altyapı hizmetleri ilk önce ayağa kaldırılır.
- Başka bir lokasyonda çalışılmasını gerektirecek bir olağanüstü durumda Kurum'a gelen çağrılar diğer ilgili lokasyonlara yönlendirilir. Ayrıca, posta yolu ile gelen evrakların da ilgili adrese iletilmesi sağlanır.

• Olağanüstü durum süresince ortaya çıkacak ek masrafları onaylamak üzere bir ya da birden fazla üst yönetici hazır bulunur.

8.2. İş Sürekliliği Senaryoları

- **Binaya Ulaşılamaması**

Kurum varlıklarına olan etkinin detaylı değerlendirilmesi:

Kurum'nin taşınmaz varlıklarının ve diğer kaynaklarının zarar görmesi durumunda, tekrar kullanılabilir duruma gelmesi için gereken zaman ve maliyetlerin değerlendirilmesidir. Tekrar kullanılabilir duruma gelemeyecek olan varlıkların/kaynakların belirlenmesi ve ilgili paydaşlarla (Yönetim Ekibi) paylaşılmasını da içerir.

Çözümün tanımlanması:

Sürecin normale dönmesi için uygulanması gereken çözüm, Kurum'nin varlıklarının ne denli etkilendiğine bağlı olarak değişir. Bu durumda uygulanacak olan çözüm detaylı bir analizin sonucunda ortaya çıkarılır.

Binaya ulaşılamaması durumunda üç farklı çözüm değerlendirilebilir:

• Eğer bina tamir edilemez bir biçimde hasar görür ya da yıkılırsa, ilk aşamada personel, İSM lokasyonunda Kurum tarafından tahsis edilmiş dizüstü bilgisayarlara kurulu VPN bağlantısı ile çalışılır.

• İhtiyaç durumunda başka bir binada yer satın alma ya da kiralama seçeneği değerlendirilir.

• Herhangi bir sebepten dolayı binaya geçici olarak ulaşılamaması durumunda, geri dönüşün sağlanabilmesi için aşağıdaki konularda gereken adımlar atılır:

• Yapısal hasar

• Su tesisatı

• İletişim

• Hijyen ve sağlık konuları

• Yapısal veya sistemsel hasarlar dışında, Kurum binasının olduğu bölgenin kapalı olması ya da kamu güvenliği tehdit eden ve geçici olarak binaya ulaşımın olmamasına yol açan durumlarda, ilk olarak durumun ne kadar süreceğine yönelik bir analiz yapılır ve uygun çözüm uygulanır.

Çözümün Uygulanması:

Binaya ulaşımın olmadığı bu senaryoda, süreçlerin devamlılığını sağlamak için yeni bir lokasyona taşınmak için aşağıdaki işlemlerin yapılması gerekmektedir.

• Telefonların yönlendirilmesi

• Süreçlerin devam etmesi için gereken evrakların, belge ve klasörlerin taşınması (Araç kiralama)

• Binaya giriş yetkilerinin tanımlanması

Devreye alınan İş Sürekliliği Planı'ndan uygun bir biçimde geri dönüş sağlanarak normal operasyonlara devam etmek gerekmektedir. Bu amaçla aşağıdaki adımlar gerçekleştirilmelidir:

• Geri dönüş prosedürlerinin oluşturulması

• Olağanüstü durumda kullanılan sistemlerden normal durumda kullanılan sistemlere dönülmesi

• Olağanüstü durumda kullanılan ekipmanların iade edilmesi

Aşağıda yer alan konulara ilişkin bilgilerin yönetilmesi kritik öneme sahiptir:

- Zarar gören insan kaynağı
- Ana ve yedekler sistemler
- Üçüncü taraflar, piyasa ve müşteriler (Önemli müşteriler)

Normal süreçlere geçiş, şartlara uygun olarak kademeli şekilde uygulanır. Hangi çözümün ve yöntemin uygulanması gerektiği, anın şartlarına ve mevcut çözümlere göre değerlendirildiği gibi aynı zamanda çözümün ayrı bir kesintiye neden olmaması/riskinin düşük olması da göz önünde bulundurulur. Kademeli olarak uygulanacak olan çözüm bu sayede Kurum'ye işlemlerin test edilmesi imkanını da sunmaktadır.

Normalleşme sürecinin takip edilmesi:

Süreçlerin normalleşmesi safhasında ve yeni temin edilen ya da onarılan kaynakların kullanılmaya başlanmasını takip eden birkaç gün, Acil Durum Ekibi ve İş Kurtarma Ekibi mevcut durumu izler ve gözlemler. Sorun yaşanması durunda en kısa sürede müdahale ve çözüme odaklanır. İzlenmesi gereken süreçlerden bazıları aşağıda belirtilmiştir:

- Bütün cihazların, ekipmanın ve iletişim sistemlerinin kontrol edilmesi
- Altyapı sistemlerinin performans değerlerinin kontrol edilmesi için koordinasyonun sağlanması

- **BT Sistem Kesintisi**

Kurum Olağanüstü Durum ağ topoloji yapısı görseli aşağıda paylaşılmıştır. Ayrıca Replikasyona giden sunucu listesi EK – 2 yer almaktadır. Kritik personeller [redacted] IP adresli fiziksel sunucuya Kurum'un kendilerine tahsis ettiği dizüstü bilgisayarlar ile VPN üzerinden Genex ve GTrader uygulama veri tabanlarına bağlantı kurarlar.

Kurum varlıklarına olan etkinin detaylı değerlendirilmesi:

Kurum'nin BT sistemlerinin kesintiye uğraması durumunda, tekrar kullanılabilir duruma gelmesi için gereken zaman ve maliyetlerin değerlendirilmesidir. Tekrar kullanılabilir duruma gelemeyecek olan varlıkların/kaynakların belirlenmesi ve ilgili paydaşlarla (Yönetim Ekibi) paylaşılmasını da içerir.

Çözümün tanımlanması:

Sürecin normale dönmesi için uygulanması gereken çözüm, Kurum'nin varlıklarının ne denli etkilendiğine bağlı olarak değişir. Bu durumda uygulanacak olan çözüm detaylı bir analizin sonucunda ortaya çıkarılır.

Bilgi Teknolojileri sistem kesintisi durumunda üç farklı çözüm değerlendirilebilir:

- Eğer kesinti uzun süreli ise durum BT birimine iletilir ve Olağanüstü Durum Merkezinden çalışmalara devam edilir.
- Kesinti durumu sadece Kurum Maltepe lokasyonunda ortaya çıkarsa kullanıcılar İSM lokasyonunda ya da internet erişiminin olduğu herhangi bir yerde Kurum tarafından tahsis edilmiş dizüstü bilgisayarlara kurulu VPN bağlantısı ile bilgi sistemleri altyapısına erişebilir.

Çözümün Uygulanması:

BT sistem kesintisinin olduğu bu senaryoda, süreçlerin devamlılığını sağlamak amacıyla Olağanüstü Durum Merkezi devreye alınacak ise global BT birimi ile iletişime geçilmelidir.

Kullanıcılar tahsis edilen yerler dışında başka bir lokasyonda çalışmalarına devam edecekler ise bu durumu ve iletişim bilgilerini birim yöneticilerine iletmeleri gerekmektedir.

Devreye alınan İş Sürekliliği Planı'ndan uygun bir biçimde geri dönüş sağlanarak normal operasyonlara devam etmek gerekmektedir. Bu amaçla aşağıdaki adımlar gerçekleştirilmelidir:

- Geri dönüş prosedürlerinin oluşturulması
- Olağanüstü durumda kullanılan sistemlerden normal durumda kullanılan sistemlere dönülmesi
- Olağanüstü durumda kullanılan ekipmanların iade edilmesi

Aşağıda yer alan konulara ilişkin bilgilerin yönetilmesi kritik öneme sahiptir:

- Zarar gören insan kaynağı
- Ana ve yedekler sistemler
- Üçüncü taraflar, piyasa ve müşteriler (Önemli müşteriler)

Normal süreçlere geçiş, şartlara uygun olarak kademeli şekilde uygulanır. Hangi çözümün ve yöntemin uygulanması gerektiği, anın şartlarına ve mevcut çözümlere göre değerlendirildiği gibi aynı zamanda çözümün ayrı bir kesintiye neden olmaması/riskinin düşük olması da göz önünde bulundurulur. Kademeli olarak uygulanacak olan çözüm bu sayede Kurum'ye işlemlerin test edilmesi imkanını da sunmaktadır.

Normalleşme sürecinin takip edilmesi:

Süreçlerin normalleşmesi safhasında ve yeni temin edilen ya da onarılan kaynakların kullanılmaya başlanmasını takip eden birkaç gün, Acil Durum Ekibi mevcut durumu izler ve gözlemler. Sorun yaşanması durunda en kısa sürede müdahale ve çözüme odaklanır. İzlenmesi gereken süreçlerden bazıları aşağıda belirtilmiştir:

- Bütün cihazların, ekipmanın ve iletişim sistemlerinin kontrol edilmesi
- Altyapı sistemlerinin performans değerlerinin kontrol edilmesi için koordinasyonun sağlanması

- **Kritik Personele Ulaşılamaması**

Kurum varlıklarına olan etkinin detaylı değerlendirilmesi:

Kritik Kurum personeline ulaşılamaması durumunda ilgili birim müdürleri/süreç sahipleri İnsan Kaynakları ile ortak bir değerlendirme yaparak ne kadar süreyle bu personele ulaşılamayacağı, yerine yeni personel istihdam edilip edilmeyeceği konusunu netleştirir.

Çözümün tanımlanması:

Sürecin normale dönmesi için uygulanması gereken çözüm, kritik personele ulaşılamamasının etkisine bağlı olarak değişir. Buradan yola çıkarak iki farklı durumu değerlendirebiliriz:

• İnsan kaynağı kalıcı olarak kullanılamayacak durumda ise, çözüm, Kurum içinden transferler ya da Kurum dışından yeni kaynakların işe alınması olacaktır.

• İnsan kaynağı geçici olarak kullanılamıyor ise, çözüm süreye bağlı olarak değerlendirilir ve uygulanır. Geçici görevlendirme (personel/birim) ya da dış kaynak kullanımı (geçici personel istihdamı) uygulanabilir çözümler arasındadır. Personel görevine geri döndüğü zaman yerine göreve getirilen kişinin/kişilerin işleri sorunsuz olarak devretmesi gerekmektedir.

Her iki seçenekte göreve getirilen yeni personel için eğitimler ve yönlendirme çalışmaları gerçekleştirilmelidir.

Çözümün Uygulanması

Kritik personele ulaşılamadığı bu senaryoda, çözümün etkin şekilde uygulandığından emin olmak için ilgili birim tarafından gerçekleştirilmesi gereken adımlar aşağıda sıralanmıştır:

• Eski kullanıcı hesabının kapatılması (geçici/kalıcı) ve yeni göreve getirilen personel için yeni kullanıcı hesabının oluşturulması ya da eski kullanıcı hesabının (varsa) güncellenmesi

• Süreçlerin devam etmesi için gereken evrak, belge ve klasörlerin yeni göreve getirilen personele verilmesi

Devreye alınan İş Sürekliliği Planı'ndan uygun bir biçimde geri dönüş sağlanarak normal operasyonlara devam etmek gerekmektedir. Bu amaçla aşağıdaki adımlar gerçekleştirilmelidir:

• İşlemleri geçici olarak yapan personelin işleri uygun şekilde devretmesi

• Yeni açılan kullanıcı hesaplarının kapatılması, güncellenen hesapların eski haline getirilmesi sistemlerden kullanıcı hesaplarının kapatılması

Aşağıdaki paydaşlara gerekli bildirimlerin yapılması önemlidir:

• İnsan Kaynakları

• Yedek birimler/yedek personel/geçici personel

• Üçüncü taraflar, piyasa ve müşteriler (önemli müşteriler)

Normal süreçlere geçiş, şartlara uygun olarak kademeli şekilde uygulanır. Hangi çözümün ve yöntemin uygulanması gerektiği, anın şartlarına ve mevcut çözümlere göre değerlendirildiği gibi aynı zamanda çözümün ayrı bir kesintiye neden olmaması/riskinin düşük olması da göz önünde bulundurulur. Kademeli olarak uygulanacak olan çözüm bu sayede Kurum'ye işlemlerin test edilmesi imkanını da sunmaktadır.

Normalleşme sürecinin takip edilmesi:

Süreçlerin normalleşmesi safhasında ve yeni temin edilen ya da onarılan kaynakların kullanılmaya başlanmasını takip eden birkaç gün, Acil Durum Ekibi ve İş Kurtarma Ekibi mevcut durumu izler ve gözlemler. Sorun yaşanması durunda en kısa sürede müdahale ve çözüme odaklanır.

10. ZARAR GÖREN LOKASYONDA FAALİYETLERİN DEVAMI

Acil Durum Ekipleri çalışma alanlarındaki hasarlı/çalışabilecek bölgeleri, hasarlı/sağlam ekipmanları belirler ve Bilgi Güvenliği Sorumlusu'na iletir. Acil ve olağanüstü durumdan etkilenen birimlerin faaliyetlerini lokasyonun hasar görmeyen, az hasarlı bölümlerinde, karar verilen başka bir lokasyonda veya uzaktan çalışma alternatifiyle sürdürmeleri mümkündür.

Olağanüstü durumun yarattığı hasar ve etkiye bağlı olarak aşağıdaki alternatiflerden uygun olanlar seçilir.

- Hasarlar ön keşfi Acil Durum Ekibi tarafından yapılarak, çalışmaya uygun katlar/bölümler belirlenir.
- Kısmen çalışmaya müsait olan katlarda/bölümlerde gerekli düzenlemeler ve tadilat işlemleri başlatılır.
- Hasarın ve durumun niteliğinde göre (enerji/ekipman/iletişim) ilgili ekipler ile temasa geçilerek destek sağlanır.
- Ekipman ve donanımlar kontrol edilerek, çalışır durumda olanlar ve iş süreçlerinin devamı için gerekli ekipmanlar temin edilir.
- Enerji sarfiyatının asgariye düşürülmesi gerekmektedir. Kritik iş süreçlerinin devamı için öngörülen ekipmanlar (yazıcı, bilgisayar, vb.) haricinde elektrik sarfeden tüm cihazlar kapatılır.
- Cep telefonları ile iletişim sağlanır.

11. PLANIN GÜNCELLENMESİ

İş Sürekliliği Planları; Kurum tarafından yıllık olarak, Kurum faaliyetleri ile organizasyonel yapıdaki değişiklikler dikkate alınarak gözden geçirilir ve gerekli değişiklikler gerçekleştirilir. Güncellemeler, iş birimleri temsilcilerinin geri bildirimlerinden yararlanılarak Bilgi Güvenliği Yöneticisi koordinasyonunda yapılır ve Yönetim Kurulu tarafından onaylanır. Güncelleme süreci tamamlandıktan sonra ilgili personel ve birimlerin haberdar olması sağlanır.

Planın güncellenmesinde aşağıdaki kriterler dikkate alınır:

- Geliştirilen yeni ürün ve hizmetler,
- Mevcut ürün, hizmet ve iş süreçlerinde gerçekleştirilen değişiklikler,
- Ürün, hizmet ve iş süreçlerinde gerçekleştirilen değişiklikler nedeniyle ortaya çıkan yeni ekipman ve altyapı ihtiyaçları,
- Çalışma yerlerindeki altyapı değişiklikleri,
- Planda yer alan personelin transferi, işten ayrılması, terfisi, adres/telefon değişikliği ya da Kurum organizasyon değişiklikleri,
- İlgili dokümanlarda ya da belgelerde meydana gelen değişiklikler,
- Hizmet alınan üçüncü tarafların, alınan hizmetlerin veya süreçlerin değişmesi,
- Test ve tatbikat sonuç raporları.

12. PLANIN SAKLANMASI VE DAĞITIMI

Kurum personelinin İş Sürekliliği Planları ile eğitime dönük diğer doküman ve bilgilere erişimi ortak alan üzerinden sağlanır. Belirtilen ana plan ile bu planı tamamlayan diğer tüm alt plan ve prosedürlerin dağıtımı Bilgi Güvenliği Sorumlusu tarafından gerçekleştirilir.

13. PLANIN YÜRÜTÜLMESİ

İş Sürekliliği Planı ve bu planı tamamlayan diğer tüm alt plan ve prosedürlerin yürütülmesi Yönetim Kurulu'nun yetki verdiği Bilgi Güvenliği Sorumlusu sorumluluğundadır.

14. REFERANSLAR / İLGİLİ DOKÜMANLAR

- EK – 1 Acil Durum, İş Kurtarma Ekipleri ve Kritik Personel Listesi
- EK – 2 Replikasyona Giden Sunucular

Hazırlayan Bilgi Güvenliği Sorumlusu	Kontrol Eden İç Kontrol Sorumlusu	YÖNETİM KURULU