Sede amministrativa – Verwaltungssitz:
Luis-Zuegg-Str. 40 I – 39012 Merano-Meran
Tel. +39 0473 498 300 – Fax +39 0473 498 303

Sede legale – Rechtssitz:
Via A.-Ammon Str. 24 I – 39042 Bressanone – Brixen
Tel. +39 0472 823 636 – Fax +39 0472 823 666
CF P.IVA St./MwSt.Nr IT/02298140217

Technisches Leistungsverzeichnis

Inhalt

1. Einleitung – Rechtsnatur, Gesellschaftszweck und Umfang der Tätigkeit der ITS GmbH 2
2. Leistungsumfang 3
2.1. Beschreibung der aktuellen Infrastruktur 3
2.2. Aktuell zugewiesene und genutzte Ressourcen 4
2.3. Anforderungen an das Rechenzentrum, das die Virtualisierungsinfrastruktur hostet 5
2.4. Anforderungen an die Virtualisierungsinfrastruktur 6
2.5. Lizenzierung der Systeme im Rechenzentrum 7
2.6. Anforderungen an das Backup-Management 8
2.7. Anforderungen an das Notfallmanagement 9
2.8. Notfall, der eine Niederlassung von ITS betrifft 10
2.9. Notfall, der das Rechenzentrum betrifft 10
2.10. Anforderungen an den Schutz vor Viren und Schadsoftware 12
2.11. Anforderungen an die Virtualisierung der Arbeitsplätze 12
2.12. Anforderungen an den Perimeterschutz des Rechenzentrums und der Niederlassungen von ITS 13
2.13. Prüfung der Sicherheit der Systeme 16
2.14. Verwaltung der Systeme von ITS im Rechenzentrum 17
2.15. Verwaltung der Client-Geräte in den Niederlassungen von ITS 18
2.16. Verwaltung von Lizenzen im Eigentum von ITS 18
2.17. Verwaltung der in den Niederlassungen von ITS eingesetzten Netzgeräte 19
2.18. Übertragung der Systeme an einen neuen Dienstleister 19
2.19. Organisation des Dienstes nach der Migration 22
3. Time & Material 23
4. Dienstgütestufen 24
5. Erweiterungen 25

1. Einleitung – Rechtsnatur, Gesellschaftszweck und Umfang der Tätigkeit der ITS GmbH

ITS GmbH ist eine Gesellschaft mit gänzlich öffentlicher Beteiligung, die nach dem Modell des „in house providing" operiert, wie es im Recht der Europäischen Union und im inländischen Recht durch Artikel 5 und 192 des GvD Nr. 50/2016, i.g.F., Artikel 4 und 16 des GvD Nr. 175/2016 i.g.F. und das LG von Bozen Nr. 12/2007 i.g.F. geregelt ist.

Als Inhouse-Gesellschaft stellt ITS Güter und Dienstleistungen bereit, die für die institutionellen Zwecke der direkt beteiligten Gesellschaften und der über diese indirekt beteiligten Verwaltungen notwendig sind (Art. 4, Absatz 1 GvD Nr. 175/2016 i.g.F.; Art. 1, Absatz 4 des LG Bozen Nr. 12/2007 i.g.F.), das heißt, sie produziert eigenständig Güter und Dienstleistungen für Zwecke der direkt beteiligten Körperschaften und der indirekt beteiligten Verwaltungen oder deren Funktionsbereiche (zweckbezogene informationstechnische Dienstleistungen) gemäß den in den EU-Richtlinien zur Vergabe öffentlicher Aufträge festgelegten Bedingungen und den einschlägigen nationalen Umsetzungsvorschriften (Art. 4, Abs. 2, Buchst. „d", und Abs. 4 GvD Nr. 175/2016 i.g.F.; Art. 1, Absatz 4 a des LG Bozen Nr. 12/2007 i.g.F.).

Die in diesem technischen Leistungsverzeichnis beschriebenen Dienstleistungen und technischen Anforderungen beziehen sich daher auf den Bedarf der ITS im allgemeinen Sinne, das heißt, unter Einbeziehung ihrer zweckbezogenen Tätigkeiten zugunsten ihrer Gesellschafterinnen, wobei auch zu berücksichtigen ist, dass die Dienstleistungen sowohl am Standort der ITS als auch an den Standorten ihrer Gesellschafterinnen erbracht werden.

Im Einzelnen werden die Dienstleistungen an folgenden Niederlassungen erbracht:

- ITS: Peter-Anich-Straße 24, 39011 Lana (BZ)
- ITS: A.-Ammon-Straße 24A, 39042 Brixen (BZ)
- ITS: Albertina-Brogliati-Straße, Nummern 8, 10, 12, 14, 39012 Meran (BZ) – NEUE NIEDERLASSUNG
- Stadtwerke Meran: Europaallee 4, 39012 Meran (BZ)
- Stadtwerke Meran: L.-Zuegg-Straße 68c 39012, Meran (BZ)
- Stadtwerke Meran: Peter-Anich-Straße 24, 39011 Lana (BZ)
- Stadtwerke Meran: Albertina-Brogliati-Straße, Nummern 8, 10, 12, 14, 39012 Meran (BZ) – NEUE NIEDERLASSUNG
- Stadtwerke Brixen: Alfred-Ammon-Straße 24, 39042 Brixen (BZ)
- Stadtwerke Brixen: c/o Acquarena, Altenmarktgasse 28/b, 39042 Brixen (BZ)
- Stadtwerke Brixen: Romstraße 9, 39042 Brixen (BZ)
- SEAB: Lancia-Straße 4/A, 39100 Bozen (BZ)

Verweise auf Niederlassungen von ITS beziehen sich im gesamten Dokument, sofern nichts anderes angegeben wird, stets auf die Niederlassungen von ITS und die an ihr beteiligten Gesellschaften; und unter der Erbringung von Dienstleistungen für ITS ist, sofern nichts anderes angegeben wird, die Erbringung von Dienstleistungen für ITS und die an ihr beteiligten Gesellschaften zu verstehen.

Die neue Niederlassung von ITS und den Stadtwerken Meran in der Brogliati-Straße in Meran wird wahrscheinlich im Laufe des Jahres 2022 eröffnet und mit einer Versetzung von Mitarbeitern und der

Überführung von Einrichtungen aus anderen Niederlassungen der beiden Körperschaften einhergehen. Eine Änderung der Gesamtzahl der Arbeitsplätze und der verwalteten Systeme, die Gegenstand dieser Ausschreibung sind, ist im Rahmen der Eröffnung der neuen Niederlassung nicht vorgesehen. Das Unternehmen, das den Zuschlag erhält, wird im Rahmen des Umzugs an der Verlagerung der Geräte, an der Neukonfiguration des Perimeterschutzes und der Einrichtung der Arbeitsplätze mitwirken und dabei auf die gemäß **Errore. L'origine riferimento non è stata trovata.** bereits vorgesehenen Ressourcen zurückgreifen.

2. Leistungsumfang

Die Ausschreibung bezieht sich auf die folgenden Leistungen:

- Bereitstellung und Betrieb der Virtualisierungsinfrastruktur für Anwendungs- und Infrastruktur-Server von ITS;
- Bereitstellung und Betrieb der Virtualisierungsinfrastruktur für virtuelle Desktops (VDI) von Workstations (PDL);
- Verwaltung und Wartung von Infrastruktur- und Anwendungsserver-Betriebssystemen;
- zentralisierte Verwaltung und Wartung der Client-Systeme an den verschiedenen ITS-Standorten;
- Bereitstellung und Verwaltung der Perimetersicherheit des Rechenzentrums;
- Bereitstellung und Verwaltung der Perimetersicherheit der ITS-Standorte, wie im entsprechenden Abschnitt benannt;
- Verwaltung der aktiven Netzausrüstung der ITS-Standorte (Switches, Router, Zugangspunkte usw.), wie im entsprechenden Abschnitt benannt;
- Systemunterstützung für die Aktivitäten anderer Anbieter an den Anwendungen und Systemen, die in der Infrastruktur von ITS vorhanden sind;
- Gewährleistung der Sicherheit der im Rechenzentrum gehosteten Daten, insbesondere durch geeignete Backup-Verfahren;
- Notfallmanagement zur Wiederaufnahme des Betriebs (Disaster Recovery) nach dem Ausfall des Rechenzentrums oder einem Notfall in einem oder mehreren Niederlassungen von ITS;
- Dokumentation der leistungen;
- Unterstützung bei der Einführung und späteren Übernahme eventueller neuer Dienste und Anwendungen, die nach der Auftragsvergabe eingeführt werden.

In den nachfolgenden Kapiteln werden die oben bezeichneten Leistungen im Detail beschrieben.

2.1. Beschreibung der aktuellen Infrastruktur

Die Infrastruktur von ITS wird aktuell im Rechenzentrum der Konverto AG mit Sitz in Bozen, Bruno-Buozzi-Straße 8, gehostet, die ihren Dienst nicht fortsetzt, und besteht aus:

- 30 dedizierten virtuellen Servern, auf denen die Infrastruktur- und Verwaltungsapplikationen von ITS gehostet sind;
- einer Infrastruktur zur Virtualisierung der Arbeitsplätze, basierend auf Citrix XenApp mit 4 für ITS dedizierten VDA-Servern (3 generische Server und 1 dedizierter Server für eine bestimmte Funktion);

- einem physischen Server (im Eigentum von ITS), der für die Oracle-Datenbank verwendet wird.

Die vom Rechenzentrum erbrachten Dienstleistungen werden in den Niederlassungen von ITS und der in den in Abschnitt **Errore. L'origine riferimento non è stata trovata.** bezeichneten beteiligten Gesellschaften über eine MPLS-Leitung und mobil oder im Smart Working über eine vom aktuellen Administrator bereitgestellte VPN-Verbindung genutzt.

2.2. Aktuell zugewiesene und genutzte Ressourcen

In Anlage A werden die aktuell im IT-System von ITS vorhandenen virtuellen und physischen Geräte, die ihnen zugeteilten Ressourcen und die Funktion der einzelnen Server detailliert beschrieben.
Insgesamt belegen die Server von ITS (mit Ausnahme der VDA-Server von Citrix) aktuell folgende virtuelle Ressourcen:

- Anzahl der Server: 30 aktive Server
- CPU: 85 zugewiesene vCPU
- RAM: 274 GB zugeteilt
- Festplattenspeicher: 8290 GB effektiv, verteilt auf 61 virtuelle Festplatten

Zusätzlich zu den erwähnten im aktuellen Rechenzentrum betriebenen Systemen ist vorgesehen, auch die zurzeit in Brixen installierte Applikation SAP in das Rechenzentrum zu verlagern. Die Migration wurde bereits begonnen und wird voraussichtlich vor Abschluss dieses Ausschreibungsverfahrens vollzogen sein. Für das SAP-System sind folgende weitere Ressourcen erforderlich:

- Anzahl der Server: 3 zusätzliche Server
- CPU: Zuweisung von 8 vCPU
- RAM: Zuteilung von 48 GB
- Festplattenspeicher: 1500 GB effektiv, verteilt auf 36 virtuelle Festplatten

Wie unten im entsprechenden Kapitel eingehend erläutert, zählen die von den Citrix VDA-Servern von Citrix beanspruchten Ressourcen nicht zu den Ressourcen von ITS, da sie als Teil der Dienstleistung betrachtet werden und folglich in der monatlichen Gebühr pro Arbeitsplatz inbegriffen sein müssen.
Um eine sachgerechte Bewertung zu ermöglichen, geben wir hier die IT-Ressourcen an, die derzeit für die Citrix VDA-Server dediziert sind:

- Anzahl der Server: 4 aktive Server
- CPU: 32 zugewiesene vCPU
- RAM: 146 GB zugeteilt
- Festplattenspeicher: 430 GB effektiv, verteilt auf 4 virtuelle Festplatten

Auf Basis der üblichen Wachstumsraten des verarbeiteten Datenvolumens und der Nutzung der Rechenressourcen schätzen wir, dass in den nächsten zwei Jahren bei gleichbleibender Anzahl der Server, einschließlich der neuen SAP-Server und ausschließlich der für Citrix dedizierten Ressourcen, insgesamt ungefähr folgende Ressourcen zugeteilt werden müssen:

- CPU: 100 vCPU
- RAM: 360 GB

- Festplattenspeicher: 12 TB

Der Zuschlagsempfänger verpflichtet sich, die im vorstehenden Absatz veranschlagten Ressourcen unverzüglich oder innerhalb von 8 Arbeitsstunden nach Anforderung im für ITS dedizierten Ressourcenpool zur Verfügung zu stellen. Die Nutzung von Ressourcen innerhalb der angegebenen Grenzen, mit Ausnahme einer Änderung der Anzahl der virtuellen Server, muss in der Monatsgebühr inbegriffen sein und darf für ITS (außer eventuellen zusätzlichen Lizenzgebühren für die Nutzung dieser Ressourcen) keine weiteren Kosten verursachen.

2.3. Anforderungen an das Rechenzentrum, das die Virtualisierungsinfrastruktur hostet

Die virtuellen und physischen Produktionssysteme von ITS müssen in einem Rechenzentrum gehostet werden, das dem Zuschlagsempfänger gehört. Sie können auch in einem Rechenzentrum eines anderen Unternehmens gehostet werden, in dem Fall jedoch nur in einem für die Systeme des Zuschlagsempfängers dedizierten Rack, dessen Zugang der Kontrolle und der Verantwortung des teilnehmenden Unternehmens unterliegt.

Das Rechenzentrum muss folgende Mindestanforderungen erfüllen:

- mindestens zwei voneinander unabhängige Stromversorgungsleitungen;
- eine Anlage zur unterbrechungsfreien Stromversorgung (UPS, Uninterruptible Power Supply) pro Versorgungsleitung zur Verhinderung einer Unterbrechung der Stromversorgung (Technologie beliebig, sofern sachgerecht dimensioniert) und zur Stabilisierung der Spannung;
- zwei Hilfsgeneratoren, die bei Problemen mit der Stromversorgung mindestens 72 Stunden lang einen autonomen Betrieb sicherstellen;
- System zur redundanten Regelung der Temperatur und Feuchtigkeit in dem Raum, in dem die Systeme, mit denen die hierin ausgeschriebenen Dienstleistungen erbracht werden, untergebracht werden sollen;
- Brandschutzsystem, das auf Rauch- und/oder Wärmesensoren basiert und mit Inertgas, Aersol oder einer gleichwertigen Technologie arbeitet, die die nicht direkt vom Brand betroffenen Einrichtungen nicht beschädigt;
- mindestens zwei voneinander unabhängige Internetverbindungen, die über unterschiedliche physische Strecken verlaufen und/oder auf unterschiedlichen Technologien basieren und von mindestens zwei verschiedenen Netzbetreibern betrieben werden;
- ein Zugangskontrollsystem, das die Nachverfolgbarkeit der physischen Zutritte von Personen zum Raum, in dem die Systeme untergebracht sind, sicherstellt und das Zutrittsprotokoll log mindestens 30 Tage lang aufbewahrt;
- ein Videoüberwachungssystem, das jeden Zutritt zum Raum, in dem die Systeme von ITS untergebracht sind, aufzeichnet und diese Videoaufzeichnungen mindestens 24 Stunden lang aufbewahrt;
- ein Alarmsystem zur Verhinderung des Eindringens unbefugter Personen;

- ein elektronisch oder mit einem Schlüssel verschließbares Rack; das Unternehmen verpflichtet sich dafür zu sorgen, dass alle Racks, in denen die Systeme von ITS untergebracht sind, auber bei Wartungsarbeiten mit einem Schlüssel verschlossen sind;
- ständige Überwachung vor Ort oder aus der Ferne, mit der Möglichkeit, auf Aufforderung innerhalb von 4 Stunden jederzeit Zutritt zu erhalten; der Zuschlagsempfänger hat anzugeben, in welcher Weise diese Aufforderung zu erfolgen hat;
- Vorliegen einer Risikoanalyse, in der alle wesentlichen Notfallrisiken und die eventuell vorgesehenen Maßnahmen zu ihrer Vermeidung und/oder Minderung untersucht werden.

Zusätzlich zu dem Hauptrechenzentrum für die Produktionssysteme muss dem Unternehmen, das den Zuschlag erhält, **– zum Zeitpunkt des Vertragsabschlusses für die gesamte Phase der Erbringung der Dienstleistungen** – ein zweites Rechenzentrum für die Wiederaufnahme des Betriebs (Disaster Recovery, DR) zur Verfügung stehen. Das Rechenzentrum für das DR kann einer Drittpartei gehören oder von dieser betrieben werden, sofern es den gleichen oben aufgeführten Anforderungen genügt wie das Produktions-Rechenzentrum.

Darüber hinaus muss das DR-Rechenzentrum den folgenden weiteren Anforderungen genügen:

- es muss mindestens 40 km Luftlinie vom Produktions-Rechenzentrum entfernt sein;
- es muss einem anderen hydrogeologischen Risiko ausgesetzt sein, als das Produktions-Rechenzentrum, zum Beispiel in einem hydrogeologisch andersartigen Gebiet liegen oder mit anderen Maßnahmen zur Risikominderung ausgestattet sein (z. B. auf erhöhtem Fundament);
- es muss einem anderen seismischen Risiko ausgesetzt sein als das Produktions-Rechenzentrum, zum Beispiel in einem seismisch andersartigen Gebiet liegen oder seismisch isoliert sein.

Das Produktions-Datenzentrum muss auf italienischem Staatsgebiet maximal 140 km von der Stadt Bozen entfernt gehostet werden, damit innerhalb angemessener Zeiträume eventuelle Arbeiten am Server vorgenommen werden können. Das DR-Rechenzentrum kann sich dagegen in einem beliebigen Land der Europäischen Union befinden. Systeme und Daten von ITS dürfen auf keinen Fall auf Systemen gespeichert oder gesichert werden, die sich außerhalb der Europäischen Union befinden, wenn sie nicht vorher nach dem AES-Verfahren mit einem mindestens 256 Bit langen Schlüssel verschlüsselt wurden.

2.4. Anforderungen an die Virtualisierungsinfrastruktur

Die Infrastruktur für die Virtualisierung der Applikations- und Infrastrukturserver von ITS muss auf der Plattform vSphere 6.7 oder höher von VMware basieren. Eine solche Plattform ist Voraussetzung für die Zertifizierung der von einigen bei ITS verwendeten Applikationen genutzten Systeme.

Die physischen Server, die die virtuellen Maschinen von ITS hosten, müssen so konfiguriert sein, dass sie vor Side-Channel-Angriffen (Spectre, Meldown usw.) geschützt sind, zum Beispiel durch Deaktivierung des Hyperthreading oder durch eigens vom Anbieter vorgesehene Konfigurationen. Alternativ kann der Dienstleister entscheiden, die physischen Server vollständig für ITS zu dedizieren oder dafür zu sorgen, dass sich auf einem physischen Host während des normalen Betriebs keine Systeme anderer Kunden befinden, mit Ausnahme der Systeme, die der Dienstleister zur

ordnungsgemäßen Erbringung der Dienstleistungen selbst benötigt (z. B. zentraler Virenschutz, VMware Management Appliance, Backup-Systeme usw.). Von dieser Regel kann nur während Wartungsarbeiten oder im Fall einer Funktionsstörung eines physischen Hosts abgewichen werden, oder wenn dies für bestimmte virtuelle Maschinen mit ITS vereinbart wurde.
Die von den Systemen von ITS genutzten virtuellen Maschinen, Netze und Datenspeicher, ausschließlich der Systeme zur Virtualisierung der Desktops, sind zu einem dedizierten Ressourcen-Pool zusammenzufassen. ITS erhält Zugriff auf das System zur Verwaltung der Virtualisierungsinfrastruktur (z. B. vCenter oder vCloud Director), mit dem es die Ressourcen des zugewiesenen Pools verwalten und ohne Einschaltung des Dienstleisters Routineaufgaben durchführen kann (Konsolen-Zugang zu den VM, Ein- und Ausschalten der Maschinen, Änderungen von RAM, CPU oder Festplatten im Rahmen des Ressourcen-Pools, Wechsel des Netzes einer VM usw.).
Die zur Desktop-Virtualisierung eingesetzten Systeme dürfen nicht zum im vorangehenden Abschnitt genannten Ressourcen-Pool gehören, können jedoch in einen anderen Ressourcen-Pool aufgenommen werden, der dediziert oder zur gemeinsamen Nutzung durch die Kunden des Zuschlagsempfängers bereitgestellt wird. ITS benötigt keinen Administrationszugriff auf die Infrastrukturserver zur Virtualisierung der Arbeitsplätze (vCenter, vCloud Director usw.).

2.5. Lizenzierung der Systeme im Rechenzentrum

Alle Lizenzen für die Virtualisierungsinfrastruktur vSphere müssen nach den Kriterien des VMware Service Provider Program (VSPP) verwaltet werden. Die Lizenzgebühren für die Betriebssysteme von Microsoft sind in die Gebühr für die virtuellen Maschinen einzubeziehen. Das Unternehmen kann sein Lizenzierungsmodell frei wählen, soweit sichergestellt ist, dass alle virtuellen Maschinen ordnungsgemäß lizenziert sind. Die Lizenzgebühren für das Betriebssystem von Microsoft sind als monatliche Kosten zulasten des Auftraggebers zu betrachten.
Die Lizenzierung der Backup-Lösung hängt von der vorgeschlagenen Lösung und der verwendeten Software ab. Der Zuschlagsempfänger garantiert, dass alle Systeme ordnungsgemäß nach den Vorgaben des Herstellers des angebotenen Produkts lizenziert sind.
Die Lizenzierung der Software zum Schutz vor Viren/antimalware hängt von der angebotenen Lösung und der verwendeten Software ab. Der Zuschlagsempfänger garantiert, dass alle Systeme ordnungsgemäß nach den Vorgaben des Herstellers des angebotenen Produkts lizenziert sind.
Die Lizenzgebühren für die virtuellen Server, die Betriebssysteme von Microsoft, die Backup-Lösung und die Software zum Schutz vor Viren und Schadsoftware müssen während der gesamten Laufzeit des Vertrags auf konstanter Höhe gehalten werden, sofern nicht die jeweiligen Anbieter ihre Lizenzierungsmodelle ändern oder ihre Lizenzgebühren um mehr als 15 % erhöhen. Wenn der Zuschlagsempfänger während der Vertragslaufzeit die Systeme für Nebendienstleistungen (Antivirus, Backup, Perimeterschutz usw.) wechseln will, muss er garantieren, dass die neuen Produkte den Anforderungen dieses Leistungsverzeichnisses genügen und durch diesen Wechsel keine Funktionsstörungen oder sonstigen Beeinträchtigungen des Auftraggebers verursacht werden.

2.6. Anforderungen an das Backup-Management

Um die Integrität und Verfügbarkeit der Daten zu sichern, müssen von allen Systemen von ITS Sicherungskopien (Backups) erstellt werden, sowohl von dem Betriebssystem als auch von den Applikationen und den zugehörigen Daten. Das implementierte Backup-System muss folgenden Anforderungen genügen:

- Die Lösung muss sowohl unter Microsoft Windows-Systemen als auch unter GNU/Linux-Systemen die Wiederherstellung der gesamten Systeme sowie einzelner in den Systemen enthaltener Dateien ermöglichen. Außerdem muss sie bei der Sicherung von Datenbanken unter Active Directory, Oracle und Microsoft SQL Server die Applikationsintegrität sicherstellen und die Wiederherstellung einzelner Objekte dieser Datenbanken ermöglichen. Für alle anderen Applikationen ist eine Gewährleistung der Ausfallsicherheit (crash consistency) ausreichend.
- Die Sicherungen müssen für alle Services mindestens täglich (einschließlich Wochenenden und an Feiertagen) vorgenommen werden. Für kritische Services können kürzere Zeitabstände für die Datensicherung festgelegt werden, jedoch nicht weniger als eine Stunde.
- Das Ergebnis der Backups muss täglich überprüft werden. Scheitert die Sicherung eines oder mehrerer Systeme und/oder Services, ist dies dem Ansprechpartner von ITS zu melden (als Alternative dazu ist dem Ansprechpartner von ITS täglich ein Bericht über das Ergebnis des Backups zuzusenden).
- Scheitert ein Backup, ist die Ursache zu ermitteln und durch geeignete Maßnahmen sicherzustellen, dass die Daten und Systeme innerhalb der darauffolgenden 24 Stunden sicher gespeichert werden können. Eventuell muss ein improvisiertes Backup durchgeführt oder vorübergehend auf ein anderes, auch manuelles, Sicherungsverfahren zurückgegriffen werden, welches sicherstellt, dass spätestens innerhalb von 48 Stunden eine neue Sicherheitskopie aller Systeme von ITS erstellt wird. Ein solcher Vorfall ist dem Ansprechpartner von ITS unverzüglich unter Angabe der Ursache und der eingeleiteten Abhilfen zu melden.
- Die Aufbewahrungsdauer der Backups aller Systeme richtet sich nach dem GFS-Schema (Grandfather, Father, Son):
  - 1 Tag bei Sicherungen in Zeitabständen von weniger als 24 Stunden,
  - 30 Tage bei Sicherungen im Zeitabstand von 1 Tag,
  - 1 Jahr bei Sicherungen im Zeitabstand von 1 Monat,
  - 5 Jahre bei Sicherungen im Zeitabstand von 1 Jahr.
- Backup-Kopien der Systeme von ITS, die nicht älter als 7 Tage sind, müssen in Online-Systemen gehostet werden, die eine schnelle Wiederherstellung der zuletzt gesicherten Daten ermöglichen und es erlauben, kritische virtuelle Maschinen direkt vom Backup-Speicherort aus neu zu starten (z. B. dedizierte NAS, Storage Appliances usw.);
- Die Backup-Kopien müssen mindestens alle 3 Tage auf ein Speichersystem übertragen oder kopiert werden, das nicht mit dem Hauptsystem verbunden ist (z. B. LTO-Bandbibliothek, VTL mit automatischer Verwaltung der Aufbewahrung, Storage Appliance mit automatisierter Snapshot-Funktion, Lösung zur Verwaltung von Cloud-Backups usw.), damit bei

elektronischen Angriffen auf die Produktionssysteme und die angeschlossenen Backup-Systeme (z. B. Diebstahl der Zugangsdaten für das Backup-System, Ransomware usw.) des Auftraggebers und/oder des Dienstleisters keine Daten verlorengehen, die älter als 4 Kalendertage sind.

- Die vorgeschlagene Backup-Lösung muss eine mindestens wöchentliche automatische Integritätsprüfung der gesicherten Kopie vorsehen. In Abstimmung mit ITS ist regelmäßig die Wiederherstellung der Backup-Sicherung zu testen:
  - Alle sechs Monate ist die vollständige Wiederherstellung einer oder mehrerer virtueller Maschinen zu testen.
  - Im monatlichen Rhythmus ist die Wiederherstellung einer oder mehrerer Dateien und/oder eines oder mehrerer Applikationsobjekte zu testen.
  - Jährlich ist die Wiederherstellung des physischen Servers mit Oracle auf einem anderen physischen Server oder auf der virtuellen Maschine zu testen und dabei zu prüfen, ob die Daten und Applikationen mit dem wiederhergestellten System einwandfrei zusammenspielen.

  Sollte wirklich einmal die Wiederherstellung eines ganzen Systems und/oder einzelner Dateien nötig sein, gilt diese innerhalb des entsprechenden Zeitraums als erprobt.

Zurzeit werden für die System-Backups insgesamt 21,5 TB genutzt. In der Dienstleistungsgebühr muss daher die Belegung von maximal 30 TB bis zum Ende des Vertrags inbegriffen sein. Auf Verlangen kann der Speicherplatz über die 30 TB hinaus in Schritten von je 100 GB erweitert werden; die im wirtschaftlichen Angebot genannte Gebühr wird dann entsprechend angepasst.
Zusätzlich zum Backup der Systeme von ITS im Rechenzentrum des Dienstleisters wird die Bereitstellung einer Backup-Lösung für die Sicherung der auf der Cloud-Plattform von Microsoft Office 365 gehosteten Daten verlangt. Insbesondere muss die vorgeschlagene Backup-Lösung alle Dokumente und Dateien von Applikationen für E-Mail-Verwaltung (Outlook), Microsoft Teams, Microsoft OneDrive und Microsoft Sharepoint sichern, die unter den Tenants von ITS und ihren beteiligten Gesellschaften gehostet sind und vom Zuschlagsempfänger verwaltet werden, und es ermöglichen, die gesicherten Daten mindestens ein Jahr lang mit einer Granularität von einem Tag aufzubewahren. Zurzeit werden für die Sicherung von Office 365-Dateien ca. 780 GB belegt. In der Dienstleistungsgebühr muss daher die Belegung von maximal 1,5 TB für Office 365 inbegriffen sein. Auf Verlangen kann der Speicherplatz über die 1,5 TB hinaus in Schritten von je 100 GB erweitert werden; die im wirtschaftlichen Angebot genannte Gebühr wird dann entsprechend angepasst.
Für Offline-Backups werden Lösungen mit austauschbaren Medien (z. B. LTO-Bänder) oder nicht überschreibbaren Medien (z. B. Appliance mit automatischem Aufbewahrungsmanagement) gegenüber traditionellen Speicherlösungen vorgezogen.
Dem Angebot sind die technischen Unterlagen beizulegen, in denen die vorgeschlagene Backup-Lösung beschrieben und dargestellt wird, dass sie oben aufgeführten Anforderungen erfüllt.

2.7. Anforderungen an das Notfallmanagement

Damit die Services auch nach Eintritt eines Notfalls weiter erbracht werden können, ist für alle im Leistungsumfang enthaltenen Services ein Notfallplan vorzubereiten.

Unter einem Notfall ist jedes Ereignis zu verstehen, das einen länger andauernden totalen oder teilweisen Ausfall der IT-Systeme des Rechenzentrums und/oder einer der in den Leistungsumfang einbezogenen Niederlassungen von ITS zur Folge hat.

2.8. Notfall, der eine Niederlassung von ITS betrifft

Sollte eine Niederlassung von ITS von einem Notfall betroffen sein, durch den die dort vorhandene in den Leistungsumfang einbezogenen IT-Geräte ganz oder teilweise verloren gehen, ist der Zuschlagsempfänger innerhalb von 72 Stunden, nachdem ihm dieser Notfall durch ITS gemeldet wurde, verpflichtet folgende Ausrüstung bereitzustellen:

- maximal 15 Arbeitsplätze in einem oder mehreren Räumen an einem Standort, der maximal 40 km von Bozen entfernt liegt,
- eine geeignete Datenverbindung zwischen dem Standort mit den Arbeitsplätzen und dem Rechenzentrum;
- maximal 10 Smart Working-Arbeitsplätze.

Jeder Arbeitsplatz muss ausgestattet sein mit:

- einem Schreibtisch;
- einem ergonomischen Stuhl;
- einem PC mit einem mindestens 15 Zoll großen Monitor, als Notebook oder als Desktop-PC mit Tastatur und Maus;
- einem Ethernet- oder WLAN-Anschluss mit Zugang zum Internet, zum Rechenzentrum und zu anderen Niederlassungen von ITS;
- Perimeterschutz mit den gleichen Merkmalen wie in den anderen Niederlassungen von ITS, auch nicht redundant konfiguriert.

Die Smart Working-Arbeitsplätze müssen ausgestattet sein mit:

- einem Notebook mit einem 14 Zoll großen Monitor, vorkonfiguriert für den Zugriff auf Services von ITS über VPN.

Die Dauer dieses Services ist auf maximal 60 Kalendertage begrenzt.

2.9. Notfall, der das Rechenzentrum betrifft

Das Unternehmen, das den Zuschlag erhält, muss dem Angebot einen Notfallplan (DRP – Disaster Recovery Plan) für die Wiederaufnahme der Services des Produktions-Rechenzentrums beilegen, das die Systeme von ITS hosten soll. Im Notfallplan ist festzulegen, welche Personen am Notfallmanagement beteiligt sind und wie das Notfallmanagement initiiert wird.

Das Notfallmanagement kann initiiert werden, wenn die Services, die ITS über das Produktions-Rechenzentrum erbringt, schätzungsweise 4 Arbeitsstunden lang nicht verfügbar sind, und in Abstimmung mit dem Personal von ITS. Im Notfallplan müssen klar die Abläufe festgelegt werden, die im Falle einer Nichtverfügbarkeit der von ITS erbrachten Services aufgrund von Ereignissen, die das Rechenzentrum oder Teile davon betreffen, einzuhalten sind. In Anhang A sind, zusammen mit der Liste der Systeme von ITS, die zulässigen Höchstwerte für die Ausfallzeit (RTO, Return To

Operation) und den Datenverlust (RPO, Recovery Point Objective) für jedes in den Leistungsumfang einbezogene System angegeben.
Die Wiederherstellung der virtuellen Server nach Notfällen erfolgt unter Nutzung einer anderen Virtualisierungsinfrastruktur, die auf der gleichen Version von VMware vSphere basiert, wie sie in der Produktion verwendet wird. Der den Systemen am vom Notfall betroffenen Standort zugewiesene Festplattenspeicher bleibt unverändert, die RAM- und CPU-Ressourcen können jedoch um 25 % beziehungsweise 50 % verringert werden, sofern die gesamte Leistung der Systeme dadurch nicht um mehr als 20 % im Vergleich zum Normalbetrieb sinkt.
Was den physischen Oracle-Server, vitsdb01, betrifft, kann der Anbieter in seinem Ermessen eine Notfallmanagementlösung implementieren, welche die Wiederherstellung auf einem anderen physischen Server oder auf einem virtuellen Server mit gleichen Ressourcen und gleicher Leistung vorsieht. Der Zuschlagsempfänger garantiert, dass bei der Wiederherstellung des physischen Servers die Lizenzbedingungen eingehalten werden, erwirbt gegebenenfalls die für die Zielsysteme nötige Lizenz oder stellt einen Backup- und Wiederherstellungsprozess bereit, der eine Wiederherstellung des Systems unter Einhaltung der in Anhang A angegebenen Höchstwerte für die Wiederherstellungszeit (RPO) und den Datenverlust (RTO) ermöglicht.
Dauert der Systemausfall länger als 15 Tage, muss der Zuschlagsempfänger die Hardware-Ressourcen am Standort des Notfalls ergänzen, um die Verfügbarkeit der Ressourcen sicherzustellen, die für die vorherigen Produktionssysteme von ITS reserviert waren.
Für den Fall, dass der Systemausfall länger als 30 Tage dauert, muss der Zuschlagsempfänger einen neuen Notfallplan vorbereiten, der die Möglichkeit eines Ausfalls im DR-Rechenzentrum berücksichtigt. Die in Anhang A festgelegten Maximalwerte RTO und RPO werden in diesem Fall auf ihr Dreifaches erhöht.
Der Dienstleister muss innerhalb von 60 Tagen nach Initiierung der DR einen „Wiederherstellungsplan“ vorlegen, in dem erläutert wird, welche Arbeiten für die Wiederinbetriebnahme des Produktions-Rechenzentrums (soweit möglich) oder dessen Wiederaufbau an einem anderen Standort nach den im Kapitel „**Errore. L'origine riferimento non è stata trovata.**“ genannten Kriterien notwendig sind. Die Wiederherstellung muss innerhalb von 120 Kalendertagen ab dem Datum der Auslösung des Notfallplans abgeschlossen sein. Falls das DR-Rechenzentrum den im entsprechenden Kapitel beschriebenen Anforderungen an das Produktions-Rechenzentrum genügt, steht es dem Zuschlagsempfänger frei, in Abstimmung mit ITS den Standort der DR zum Standort der Produktion zu machen und gleichzeitig ein neues DR-Datenzentrum bereitzustellen, das allen in diesem Leistungsverzeichnis niedergelegten Vorschriften genügt, und die für die Produktionssysteme erforderlichen Ressourcen wiederherzustellen.
Die mit der Wiederaufnahme des Betriebs und der Wiederherstellung durch den Dienstleister verbundenen Kosten gehen vollständig zu dessen Lasten; ITS ist in diesem Fall von jeglicher Haftung freigestellt.

2.10. Anforderungen an den Schutz vor Viren und Schadsoftware

Alle Server, die Gegenstand der Dienstleistung sind, müssen mit einem Schutz vor Viren und Schadsoftware ausgestattet sein, sofern ITS in der Phase der Dienstleistungserbringung keine andere Weisung erteilt. Der Virenschutz kann nach Ermessen des Anbieters durch eine auf jedem virtuellen Server installierte Software (einen Agenten) gewährleistet oder in das Virtualisierungssystem (agentenlos) integriert werden. Für den physischen Oracle-Server muss zwingend eine agentenbasierte Lösung gewählt werden. Der gewählte Virenschutz muss über eine zentrale Schnittstelle mit rollenbasierter Zugriffskontrolle verwaltet werden können. Ferner muss ITS ein Satz von Zugangsdaten zur Verfügung gestellt werden, der es zuständigen Mitarbeitern ermöglicht, selbst den Virenschutzstatus der einzelnen Systeme und die eventuell abgefangenen Bedrohungen zu prüfen.

Zusätzlich zur Virenschutzlösung für die virtuellen Server muss der Dienstleister eine Viren- und Malwareschutzlösung für den physischen Oracle-Server und für alle physischen Arbeitsplätze – Desktops, Notebooks oder Mobilgeräte – bei ITS und den Stadtwerken Meran bereitstellen. In dieser ersten Phase werden die Stadtwerke Brixen und die SEAB nicht in den zentralisierten Viren- und Malwareschutz einbezogen, können jedoch in naher Zukunft hinzugefügt werden. Wie bei den virtuellen Servern muss das gewählte Produkt über eine zentrale Konsole mit rollenbasierter Zugriffskontrolle verwaltet werden können. Sofern hierfür nicht die Verwaltungsschnittstelle des Virenschutzsystems für die virtuellen Server verwendet wird, muss auch für diese Konsole ITS ein Zugangsdatensatz zur Verfügung gestellt werden, der es zuständigen Mitarbeitern ermöglicht, selbst den Virenschutzstatus der einzelnen Systeme und die eventuell abgefangenen Bedrohungen zu prüfen.

Die vorgeschlagene Virenschutzlösung für die virtuellen Server kann sich von der für die physischen Arbeitsplätze der Benutzer unterscheiden. Gegebenenfalls kann das Virenschutzprodukt für die physischen Client-Plätze in das Perimeterschutzsystem integriert werden, sodass die Sicherheit der Netze von ITS dann durch ein einziges System kontrolliert wird.

Die Lizenzierung der Lösung für die Serversysteme muss der Dienstleister nach dem Lizenzierungsmodell des Lieferanten des Produkts vornehmen und verwalten. Die Lizenzgebühr für das Viren- und Malwareschutzprodukt für die Server ist, soweit vorgesehen, in die Monatsgebühr für jede Maschine einzubeziehen.

Die Lizenzierung der Lösung für die physischen Client-Plätze muss der Dienstleister nach dem Lizenzierungsmodell des Lieferanten des Produkts vornehmen und verwalten. Die Lizenzierungsgebühr ist im Angebot in die Monatsgebühr für jede Maschine einzubeziehen.

2.11. Anforderungen an die Virtualisierung der Arbeitsplätze

Zur Verwaltung der virtualisierten Arbeitsplätze wird zurzeit die Citrix-Plattform des aktuellen Dienstleisters verwendet. ITS sind zurzeit 4 virtuelle Server zugewiesen, die das Produkt XenApp nutzen, um insgesamt 66 virtuelle Arbeitsplätze bereitzustellen, von denen normalerweise 40-45

gleichzeitig aktiv sind. Von den 4 vorhandenen VDA-Servern sind 3 generische Server, die den Nutzern alle Basisapplikationen zur Verfügung stellen, während ein Server exklusiv für die Applikation WinSmart dediziert ist, die für die Waage im Recycling-Zentrum verwendet wird.
Die vorgeschlagene Lösung zur Virtualisierung der Arbeitsplätze muss auf der Citrix-Plattform, in der Version XenApp oder XenDesktop oder einer Kombination aus diesen beiden Lösungen, basieren. Die Infrastrukturserver für die Lösung (z. B. Access Gateway, Storefront, Delivery Controller, Lizenzserver, SQL Server usw.) können ITS dediziert oder mit anderen Kunden geteilt werden, während die VDA-Server (Virtual Delivery Agent) ITS dediziert bereitgestellt werden müssen. Der Zugriff der Benutzer auf die Systeme muss auf Basis der Active Directory-Nutzerdatenbank von ITS erfolgen; alle Daten der Nutzer, einschließlich ihrer Zugangsdaten und ihres Benutzerverzeichnisses, sind auf dem Fileserver von ITS (vitsfs01) so zu hosten, dass jeder Benutzer unabhängig davon, mit welchem Server er sich verbindet, seine eigene Benutzerumgebung vorfindet und auf seine Daten zugreifen kann.
Die Software-Produkte, die an allen Arbeitsplätzen verfügbar sein müssen, sind in Anhang B aufgeführt. Die Lizenzen für die an den Arbeitsplätzen verwendeten Applikationen sind aktuell Eigentum von ITS und können auch auf der neuen Infrastruktur genutzt werden. Auch die Lizenzen etwaiger neuer Produkte, die während der Vertragslaufzeit installiert werden müssen, werden von ITS erworben (sofern das Lizenzmodell der gewählten Software dies zulässt) und dem Dienstleister zur Verfügung gestellt.
Die Lizenzierung der Infrastruktur der virtuellen Arbeitsplätze muss, mit Ausnahme der im vorherigen Abschnitt erwähnten Software-Lizenzen, gemäß den Lizenzierungsmodellen von Citrix vorgenommen werden, unter Einbeziehung der virtuellen Maschinen, der Betriebssysteme und der Lizenzen für Microsoft RDS.
Die Kosten für die virtuellen Arbeitsplätze sind als allumfassende Monatsgebühr für die IT-Ressourcen und die Lizenzen zu berücksichtigen, unabhängig von der Anzahl der erforderlichen virtuellen Desktops, der Anzahl der zur Erbringung des Service verwendeten virtuellen Maschinen und der diesen zugeteilten Ressourcen. Insbesondere sind die Service-Kosten der virtuellen Desktops, einschließlich die Kosten der genutzten virtuellen Ressourcen, der Kosten der Lizenzierung der virtuellen VDA-Server, des Betriebssystems, der Remote-Desktop-Verbindungen, der Datensicherung, des Virenschutzes, der regelmäßigen Wartung der Systeme, in die einheitliche Monatsgebühr für jeden virtualisierten Arbeitsplatz einzubeziehen.

2.12. Anforderungen an den Perimeterschutz des Rechenzentrums und der Niederlassungen von ITS

Für den Perimeterschutz des Rechenzentrums und der Niederlassungen von ITS muss der Zuschlagsempfänger eine Lösung auf Basis von Firewall-Produkten der nächsten Generation (Next Generation Firewall, NGFW) implementieren, welche die Funktionalität UTM (Unified Threat Protection) beinhalten und die Implementierung einer SD-WAN-Lösung nativ unterstützen.
Die zu implementierende Lösung beruht auf einer oder mehreren physischen oder virtuellen Instanzen, die den Systemen von ITS im Rechenzentrum zugewiesen sind, und auf einer oder mehreren physischen oder virtuellen Instanzen für die Niederlassungen, in denen sich die

Arbeitsplätze von ITS befinden. Alle Instanzen müssen redundant konfiguriert sein, damit die Funktion der Sicherheits-Services auch dann sichergestellt ist, wenn die Hardware eines Geräts oder des Virtualisierungssystems, das die virtuelle Instanz unterstützt, defekt ist. Alle physischen und/oder virtuellen Instanzen werden über eine zentrale, über das Internet mit einem Browser zugängliche Schnittstelle verwaltet. ITS erhält mindestens einen Zugangsdatensatz, um die implementierten Richtlinien und Protokolle der Firewalls im Rechenzentrum und in den Niederlassungen kontrollieren zu können.

Die vorgeschlagenen Firewalls müssen die klassischen und die erweiterten Firewall-Funktionen NGFW und UTM unterstützen und insbesondere folgenden Anforderungen erfüllen:

- SSL Inspection zur Prüfung verschlüsselter Inhalte, anwendbar mindestens für Services für Internetnavigation (HTTP), E-Mail (SMTP, IMAP, POP3) und Secure Shell (SSH);
- äußerer Virenschutz, der den gesamten unverschlüsselten und verschlüsselten (SSL/TLS) Internet- und E-Mail-Verkehr (HTTP bzw. SMTP, IMAP und POP3) analysiert;
- Anwendungskontrolle, die es ermöglicht, Richtlinien auf Basis der Erkennung der wichtigsten von ITS verwendeten Applikationen festzulegen (z. B. Microsoft Office365, Microsoft Teams, Citrix ICA, Autodesk 360, Adobe Creative usw.), unabhängig von verwendeten Protokollen und Ports;
- Funktionalitäten IDS (Intrusion Detection System) und IPS (Intrusion Prevention System), mit denen sich Bedrohungen erkennen und abwehren lassen, die Schwachstellen der geschützten Systeme ausnutzen, sowie eventuelle Angriffe aus dem Internet oder aus den Netzen von ITS oder der Partner;
- Integration in Microsoft Active Directory, damit die Benutzer erkannt werden und Richtlinien für bestimmte Benutzer oder Benutzergruppen festgelegt werden können, sowohl für physische Clients als auch für die virtuelle Desktop-Umgebung. Möglichkeit, die Benutzerdatenbank Active Directory auch zur Authentifizierung von VPN zu nutzen;
- Filterung des Internet-Verkehrs nach Inhaltskategorien, sodass Websites mit bestimmten Inhalten (z. B. Pornografie, unsichere Websites, Glücksspiele usw.) blockiert werden können, mit der Möglichkeit, diese Filterung je nach Benutzergruppe unterschiedlich zu konfigurieren;
- Content Filtering zur Blockierung oder Zulassung bestimmter Datentypen (zum Beispiel zum Erkennen ausführbarer Dateien) und optional DLP (Data Leakage Prevention) zum Erkennen und/oder Abwehren von Versuchen, vertrauliche oder geschützte Daten aus dem Unternehmen herauszuschleusen;
- Unterstützung der Festlegung von FQDN (Fully Qualified Domain Name) als Quell- oder Zieladresse in den Filterungsrichtlinien;
- Unterstützung der Steuerung der Dienstgüte (Quality of Service, QoS) und des Traffic Shaping zur Priorisierung des Datenverkehrs nach Datentypen und/oder Benutzergruppen;
- Unterstützung des Fernzugriffs von Benutzern und Dienstleistern von ITS über VPN. Der VPN-Dienst, oder zumindest seine Basisfunktionen, müssen auch im Clientless-Modus genutzt werden können, das heißt, allein mit einem Web-Browser, ohne dass ein spezieller VPN-Client auf dem zu verbindenden Gerät installiert werden muss, und/oder über ein Portal, und mindestens die Protokolle RDP, VNC, SSH und TELNET unterstützen;

- Unterstützung von IPsec VPN Site to Site über die Protokolle IKEv1 und IKEv2;
- Unterstützung der SD-WAN-Funktionalität zur dynamischen Verwaltung der zahlreichen WAN-Verbindungen (nach Qualität, Zuverlässigkeit und Applikation);
- Unterstützung der Verwaltung von VPN-Verbindungen – sowohl Full Mesh als auch Hub&Spoke – zwischen den Niederlassungen von ITS und dem Rechenzentrum, einschließlich Mehrfachverbindungen und Verbindungen unterschiedlichen Typs in den verschiedenen Niederlassungen, und auch bei dynamischer öffentlicher IP-Adressierung;
- Unterstützung des Protokolls Ipv6;
- Unterstützung der dynamischen Routing-Protokolle OSPFv2 und OSPFv3 und von Policy Based Routing (PBR).

Alle im Rechenzentrum oder in den Niederlassungen für den Perimeterschutz verwendeten Geräte – sowohl Hardware als auch Software und Lizenzen – sind als Service bereitzustellen, der in der monatlichen Gebühr mit abgegolten wird.

In der Phase der Dienstleistungserbringung ist ein Arbeitstag vorzusehen, an dem die technischen Mitarbeiter des Dienstleisters mit den Ansprechpartnern von ITS festlegen, welche Sicherheitsregeln in den Perimeterschutzsystemen zu implementieren sind. Außerdem ist mindestens einmal jährlich ein weiterer halber Arbeitstag vorzusehen, an dem gemeinsam geprüft wird, ob die Richtlinien den Anforderungen des Auftraggebers entsprechen.

Die Kosten für die VPN der Benutzer von ITS sind in die Monatsgebühr für die virtuellen Arbeitsplätze einzubeziehen, während die VPN für Dienstleister und Benutzer, die nicht zu ITS gehören, in die Monatsgebühr für 10 VPN einzubeziehen sind, die ITS frei für Dienstleister oder Mitarbeiter verwenden kann. Die Kosten für jedes über diese 10 VPN hinausgehende weitere VPN sind im Angebot anzugeben.

Die neuen Perimeter-Firewalls sollen in folgenden Niederlassungen installiert werden:

- ITS: Peter-Anich-Straße 24, 39011 Lana (BZ) – 5 Benutzer
- Stadtwerke Meran: Europaallee 4, 39012 Meran (BZ) – 60 Benutzer
- Stadtwerke Meran: L.-Zuegg-Straße 68c 39012, Meran (BZ) – 5 Benutzer
- Stadtwerke Meran: Peter-Anich-Straße 24, 39011 Lana (BZ) – 20 Benutzer
- Stadtwerke Brixen: Alfred-Ammon-Straße 24, 39042 Brixen (BZ) – 80 Benutzer

Neben den Adressen ist für jede Niederlassung jeweils die ungefähre Anzahl der Benutzer des IT-Systems angegeben.

Während der Laufzeit des Vertrags ist die Überprüfung der Konnektivität zwischen dem Rechenzentrum, ITS und den Niederlassungen der beteiligten Gesellschaften vorgesehen, die im Moment in einem dedizierten MPLS-Netz besteht. Bei der Gelegenheit wird geprüft, ob sich anstelle des dedizierten MPLS die Funktionalitäten SD-WAN und VPN zusammen verwenden lassen. Die Hardware- und Softwarekonfiguration der Firewalls sind daher bereits auf diese eventuelle zukünftige Änderung vorzubereiten.

Außerdem wird wahrscheinlich im ersten Jahr der Laufzeit des Vertrags die neue Meraner Niederlassung der Stadtwerke und von ITS in Meran eröffnet. Bei der Gelegenheit müssen die in den Niederlassungen von ITS (Lana) und den Stadtwerken Meran in der Europaallee installierten Systeme an den neuen Standort verlagert und entsprechend neu konfiguriert werden. Für diese Arbeiten wird

der Auftraggeber die im Abschnitt **Errore. L'origine riferimento non è stata trovata.** aufgeführten Ressourcen einsetzen.

2.13. Prüfung der Sicherheit der Systeme

Um die Sicherheit der Daten und Systeme von ITS zu garantieren, führt der Auftraggeber mit eigenen Ressourcen und/oder unter Hinzuziehung externer Dienstleister regelmäßig ein Sicherheits-Audit und eine Schwachstellenanalyse (Vulnerability Assessment, VA) der Systeme durch. Der Zuschlagsempfänger verpflichtet sich, das Sicherheits-Audit und die Schwachstellenanalyse der Systeme von ITS zuzulassen und insbesondere Folgendes zu ermöglichen:

- die Installation virtueller Server in der Infrastruktur des Rechenzentrums zur ständigen Überwachung der Sicherheit (diese etwaigen Server werden nicht vom Zuschlagsempfänger, sondern von ITS oder anderen Dienstleistern verwaltet);
- eine eventuelle Installation von Agenten auf den Systemen von ITS, die mit Systemen innerhalb und außerhalb des Rechenzentrums kommunizieren können, um eventuelle Sicherheitsprobleme zu identifizieren;
- die Möglichkeit zur Durchführung einer Schwachstellenanalyse über das Internet zu den öffentlichen Adressen der Systeme von ITS;
- die Möglichkeit zur Durchführung einer Schwachstellenanalyse über interne Server der Infrastruktur zu den anderen ITS zugewiesenen virtuellen oder physischen Servern.

ITS verpflichtet sich, dem Dienstleister mindestens 7 Tage im Voraus mitzuteilen, an welchem Tag die Schwachstellenanalyse stattfindet und welche Systeme ihr unterzogen werden, damit er die nötigen Vorkehrungen treffen kann (z. B. Deaktivieren von IDS und IPS für bestimmte IP-Adressen, um Fehlalarme zu vermeiden). Außerdem werden dem Dienstleister der Beginn und das Ende der Schwachstellenanalyse mitgeteilt.

Die Systeme, die mit anderen Kunden geteilt werden, und insbesondere die Server zur Verwaltung der virtuellen Desktops, sind nicht Gegenstand der von ITS durchgeführten Schwachstellenanalyse; der Zuschlagsempfänger ist jedoch verpflichtet, mindestens alle sechs Monate eine Schwachstellenprüfung der Systeme durchzuführen, unter Einbeziehung aller in der CVE-Datenbank (Common Vulnerability and Exposures, https://cve.org) erfassten Schwachstellen, welche die Systeme betreffen und maximal 7 Tage vor der Schwachstellenprüfung erfasst wurden.

Innerhalb von 15 Tagen nach Durchführung der Schwachstellenprüfung der gemeinsam genutzten Systeme ist ITS ein Bericht vorzulegen, der bezüglich aller Schwachstellen, die im CVSS (Common Vulnerability Scoring System) mit einer höheren Punktzahl als 4 (also mit Medium, High oder Critical) eingestuft sind, den Anfälligkeitsstatus der Systeme sowie die geplante Behebung und/oder Minderung dokumentiert.

Die von ITS oder beauftragten Dienstleistern durchgeführten Audits und die Schwachstellenprüfungen werden nach Möglichkeit so durchgeführt, dass sie die Services nicht beeinträchtigen. Für den Fall, dass nach oder infolge der Durchführung eines Audits und/oder einer Schwachstellenprüfung Funktionsstörungen in den Systemen von ITS auftreten, ist der Dienstleister diesbezüglich von jeglicher Haftung freigestellt, und die etwaigen Kosten zur Wiederaufnahme der Services gehen zulasten von ITS.

2.14. Verwaltung der Systeme von ITS im Rechenzentrum

Der Zuschlagsempfänger muss in seinem wirtschaftlichen Angebot alle Tätigkeiten zur laufenden Verwaltung der Systeme von ITS im Rechenzentrum in der Servicegebühr berücksichtigen. Insbesondere sind folgende Tätigkeiten in die Servicegebühr einzubeziehen:

- Überwachung der Ressourcennutzung und der korrekten Serviceleistung durch die Systeme (Basismonitoring der CPU, des RAM, der Nutzung des Festplattenspeichers, der aktiven Applikationsdienste usw.);
- ordentliche Systemwartung (Bereinigung, regelmäßige Neustarts usw.);
- Aktualisierung der Betriebssysteme mit den neuesten Sicherheits-Patches;
- Aktualisierung der auf der Virtualisierungsplattform der Arbeitsplätze installierten Applikationen;
- Kontrolle der Datensicherung und eventuell erforderliche Korrekturmaßnahmen;
- Kontrolle des Virenschutzes und eventuell erforderliche Korrekturmaßnahmen;
- Verwaltung der Active Directory-Benutzerdatenbank;
- Festlegung und Pflege der Active Directory-Richtlinien (GPO);
- Erstellen neuer virtueller Maschinen;
- Erstellen und Entfernen von Snapshots von virtuellen Maschinen für Arbeiten am System;
- Überwachen und Verwalten der auf den Servern installierten SSL-Zertifikate und Benachrichtigung mindestens 15 Tage vor ihrem Verfall (neue SSL-Zertifikate erwirbt ITS gegebenenfalls direkt).

In Hinblick auf die Einrichtung neuer virtueller Server müssen die Tätigkeiten für die Erstellung neuer virtueller Maschinen sowie die eventuelle Konfiguration der für deren Funktion nötigen virtuellen Infrastruktur (z. B. die Definition neuer Portgruppen auf den Virtual Switches) in die monatliche Service-Grundgebühr einberechnet werden. Nicht in die Service-Grundgebühr einbezogen sind dagegen die Tätigkeiten für die Installation und Erstkonfiguration des Systems, also die Installation des Betriebssystems, die Aktualisierung mit den neuesten Patches des Herstellers, der Beitritt zu einer Active Directory-Domäne, sofern vorgesehen, die Installation des Virenschutzprogramms und die Konfiguration des Backups der virtuellen Maschine im Backup-System. Für Arbeiten der Erstinstallation und -konfiguration ist im Angebot ein Pauschalpreis festzulegen, der während der gesamten Laufzeit des Vertrags unverändert bleibt.

Nicht in die Monatsgebühr einbezogen sind von ITS angeforderte außerordentliche Verwaltungsarbeiten wie Systemsupport für Lieferanten von Applikationen, die Durchführung von außerordentlichen Backups und/oder Wiederherstellungen wegen Arbeiten an den Systemen, die Unterstützung bei Problemen, die bei Arbeiten von Drittanbietern auftreten usw. Für Arbeiten, die nicht mit der monatlichen Servicegebühr abgegolten sind, kann ITS in eigenem Ermessen auf die in Kapitel **Errore. L'origine riferimento non è stata trovata.** genannten Ressourcen zurückgreifen.

2.15. Verwaltung der Client-Geräte in den Niederlassungen von ITS

Der Zuschlagsempfänger muss alle Tätigkeiten zur laufenden Verwaltung der physischen Client-Plätze von ITS in der Servicegebühr berücksichtigen. Zurzeit befinden sich insgesamt etwa 40-45 physische Arbeitsplätze verteilt in verschiedenen Niederlassungen von ITS und ihren beteiligten Gesellschaften.

Insbesondere sind folgende Tätigkeiten in die Servicegebühr einzubeziehen:

- die laufende Verwaltung von Thin Clients, Desktop-PCs und Notebooks, insbesondere die Aktualisierung der Systeme und Basisapplikationen und die Prüfung eventueller Meldungen der Virenschutz-/Malwareschutz-Programme;
- Fernsupport der ersten Ebene für die Benutzer bei Systemproblemen;
- Festlegung und Pflege der Active Directory-Richtlinien (GPO);
- Einrichten etwaiger neuer Arbeitsplätze oder Neuzuweisung bestehender Arbeitsplätze.

Um eine optimale Verwaltung des Maschinenparks sicherzustellen, muss der Zuschlagsempfänger ein System zur Verwaltung und Inventarisierung der in den verschiedenen Niederlassungen vorhandenen Geräte erstellen (PC, Thin Clients, Notebooks, Mobilgeräte usw.), das es ermöglicht, die gesamte installierte Software mit ihren jeweiligen Versionen, den Aktualisierungsstatus der Systeme und die Verteilung der Software und/oder Updates auf die verwalteten Systeme zu kontrollieren und die Geräte zu überwachen. Das System soll auch zur Inventarisierung und Verwaltung der Systeme im Rechenzentrum verwendet werden können. Das Verwaltungs- und Inventarisierungssystem muss ITS zugänglich gemacht werden, damit ITS eigenständig den Status der Systeme kontrollieren und die Aktualisierung der Client-Systeme verwalten kann.

Außerordentliche, von ITS gesondert angeforderte Verwaltungstätigkeiten und etwaige Arbeiten an Client-Plätzen, die nicht aus der Ferne durchgeführt werden können, sind nicht in der Monatsgebühr inbegriffen. Für Arbeiten, die nicht mit der monatlichen Servicegebühr abgegolten sind, kann ITS in eigenem Ermessen auf die in Kapitel **Errore. L'origine riferimento non è stata trovata.** genannten Ressourcen zurückgreifen.

2.16. Verwaltung von Lizenzen im Eigentum von ITS

Der Zuschlagsempfänger muss in seinem finanziellen Angebot alle Tätigkeiten zur Verwaltung der im Eigentum von ITS befindlichen Lizenzen für die Systeme berücksichtigen, die Gegenstand dieses technischen Leistungsverzeichnisses sind, sowohl die Systeme im Datenzentrum als auch die Systeme in den verschiedenen Niederlassungen. Insbesondere übernimmt der Zuschlagsempfänger auf Rechnung von ITS folgende Tätigkeiten:

- Verwaltung der Microsoft-Tenants für Office365;
- Verwaltung der Lizenzen von Microsoft für die Arbeitsplätze;
- Verwaltung der Lizenzen für die auf den virtuellen Desktops installierten Applikationen;
- etwaige Beratung zur Verwaltung der Lizenzen für die auf den Systemen des Rechenzentrums installierten Applikationen.

Die Verwaltung der Lizenzen beinhaltet die Unterstützung bei der Registrierung neuer Lizenzen, die Prüfung, ob die verfügbaren Lizenzen der installierten Software entsprechen, die Abtretung nicht mehr erforderlicher Lizenzen und weitere Tätigkeiten, die in dem Zusammenhang während der Vertragslaufzeit notwendig sind. Die Beratung kann sich im Wesentlichen auf Strategien zur Einsparung von Lizenzgebühren für Systeme und Applikationen und auf entsprechende strukturelle oder organisatorische Änderungen auf Seiten des Auftraggebers beziehen. Zurzeit sind zwei Microsoft Office365 Tenants eingerichtet, jeweils einer für ITS und für die Stadtwerke Meran.

2.17. Verwaltung der in den Niederlassungen von ITS eingesetzten Netzgeräte

Der Zuschlagsempfänger muss alle nicht vom Netzbetreiber übernommenen Tätigkeiten zur laufenden Verwaltung der in den Niederlassungen von ITS eingesetzten Netzgeräte in der Servicegebühr berücksichtigen. Insbesondere übernimmt der Zuschlagsempfänger auf Rechnung von ITS sämtliche Arbeiten zur Verwaltung und Konfiguration der in den Niederlassungen vorhandenen Geräte, insbesondere:

- die Aktualisierung der Systeme;
- die Speicherung der Konfigurationen;
- die Änderung der Konfigurationen auf Verlangen von ITS.

Ausgenommen sind Arbeiten zur Konfiguration und Installation neuer Geräte und im Zusammenhang mit dem Austausch etwaiger schadhafter Geräte. In den Geltungsbereich dieses Leistungsverzeichnisses fallen zurzeit folgende Geräte:

- 10 Switches;
- 4 Router;
- 20 Access Points.

Für Arbeiten, die nicht mit der monatlichen Servicegebühr abgegolten sind, kann ITS in eigenem Ermessen auf die in Kapitel **Errore. L'origine riferimento non è stata trovata.** genannten Ressourcen zurückgreifen.

2.18. Übertragung der Systeme an einen neuen Dienstleister

Die Übertragung der Systeme vom aktuellen Verwalter an den Zuschlagsempfänger muss innerhalb von 60 Tagen nach Abschluss des Vertrags erfolgen und darf über das in dieser Ausschreibung Festgelegte hinaus mit keinen weiteren Belastungen von ITS verbunden sein.
Der Zuschlagsempfänger verpflichtet sich, innerhalb von 30 Tagen nach Abschluss des Vertrags einen Migrations-Projektplan zu erstellen, in dem alle Schritte zur Übertragung der Systeme vom aktuellen Rechenzentrum auf das neue Rechenzentrum dargestellt sind, insbesondere die Aktivitäten, welche die Mitwirkung von ITS erfordern, eine Unterbrechung der Dienste von ITS bewirken oder Maßnahmen des aktuellen Dienstleisters notwendig machen.

In diesem Projektplan ist anzugeben, an welchem Tage die Migration abgeschlossen sein soll; ferner sind darin in einem Gantt-Diagramm die einzelnen Maßnahmen mit den jeweils beteiligten Parteien aufzuführen.
Alle Aktivitäten, die in einer oder mehreren Niederlassungen zu einem allgemeinen Ausfall der Dienste führen können, sind außerhalb der Arbeitszeiten durchzuführen, das heißt, Montag bis Donnerstag zwischen 18:00 Uhr und 07:00 Uhr des Folgetages oder Freitag 13:00 Uhr bis Montag 07:00 Uhr. Etwaige Ausfälle während der Geschäftszeiten begründen Vertragsstrafen. Für die gegebenenfalls nötige Neukonfigurierung der physischen Clients der Benutzer wird eine Ausfallfallzeit von maximal 30 Minuten pro Arbeitsplatz eingeräumt, sofern sich diese Neukonfiguration nicht aus der Ferne und außerhalb der Arbeitszeiten durchführen lässt. Im Migrationsplan sind die geplanten Arbeiten aufzuführen. Eventuelle Maßnahmen vor Ort an den Arbeitsplätzen werden unter Berücksichtigung der Anforderungen der betroffenen Dienste gemeinsam mit ITS geplant (zum Beispiel sollten Arbeitsplätze mit gleichen Funktionalitäten möglichst nicht gleichzeitig aktualisiert werden).
ITS hat dem Zuschlagsempfänger, wenn dieser es für nötig oder zweckmäßig hält, auf Verlangen eine vollständige Kopie der letzten Backups der Systeme von ITS auf einem vom Zuschlagsempfänger gelieferten Datenträger (HDD oder NAS) in dem Format zur Verfügung zu stellen, das vom aktuell verwendeten Produkt Veeam Backup & Recovery Version 10 verwendet wird. Die Backups sind innerhalb von 7 Tagen ab der tatsächlichen Verfügbarkeit des Datenträgers zur Verfügung zu stellen. Die Kosten, die für diese Maßnahme dem aktuellen Dienstleister zu erstatten sind, gehen zulasten von ITS.
Wenn der Zuschlagsempfänger es für nötig oder zweckmäßig hält, kann zwischen der Infrastruktur des Rechenzentrums am Standort des aktuellen Dienstleisters und der Infrastruktur des Rechenzentrums am Zielort eine VPN IPSec-Verbindung eingerichtet werden. Die Nutzung der VPN-Verbindung darf die Benutzer von ITS in keiner Weise an der Nutzung der Dienste hindern (insbesondere dürfen keine Datentransfers vorgenommen werden, die das von ITS zur Bereitstellung seiner Dienste zur Verfügung stehende Band vollständig belegen können). Die Kosten für die Einrichtung der VPN IPSec-Verbindung durch den aktuellen Dienstleister gehen zulasten von ITS:
Auf Verlangen wird für Zwecke der Migration ein Zugangsdatensatz für den Administratorzugriff auf alle Systeme von ITS bereitgestellt, die Gegenstand der Ausschreibung sind.
Der Zuschlagsempfänger übernimmt die Bereitstellung der Lösung zur Virtualisierung der Arbeitsplätze und sorgt für die Installation der vorgeschlagenen Lösung mit allen in Anhang B bezeichneten Applikationen. Der Zuschlagsempfänger verpflichtet sich zudem, mindestens 10 Tage vor dem angegebenen Abschlusstermin der Migration einen Test-Arbeitsplatz bereitzustellen, damit die Mitarbeiter von ITS die ordnungsgemäße Funktion der neuen Arbeitsplätze überprüfen und eventuelle Probleme beheben können.
Der Zuschlagsempfänger übernimmt die Verlagerung des ITS gehörenden physischen Servers mit Oracle vom aktuellen Rechenzentrum in das neue Rechenzentrum, insbesondere die Demontage, den Transport, den Aufbau des Servers am neuen Standort und die Durchführung der Funktionstests. ITS garantiert, dass das System ordnungsgemäß abgeschaltet ist und eine Sicherungskopie der zum Zeitpunkt der Abschaltung auf dem Server vorhandenen Daten existiert. Eventuelle Probleme während der Verlagerung des Servers (z. B. Beschädigung während des Transports oder bei

Abbau/Aufbau) sind vom Zuschlagsempfänger zu beheben. Der Zuschlagsempfänger muss im Rahmen seiner Möglichkeiten dafür sorgen, dass die Dienste am folgenden Arbeitstag ordnungsgemäß erbracht werden können, zum Beispiel indem er Ersatzhardware zur Verfügung stellt, ohne dass ITS dadurch zusätzliche Kosten entstehen.

Die virtuellen Server müssen gemäß den Vorgaben des Migrations-Projektplans des Zuschlagsempfängers von der aktuellen Infrastruktur zur Infrastruktur des Zuschlagsempfängers migriert werden. Die Migration kann in beliebiger Weise erfolgen, zum Beispiel durch Backup und Wiederherstellung, Online-Migration, Synchronisierung der Systeme über das Netzwerk, Installation neuer Server und Verlagerung der Daten usw. Der Zuschlagsempfänger muss sich, je nach gewählter Methode der Migration, vergewissern, dass eventuelle Änderungen an den Systemen nicht deren Kompatibilität mit den von ITS installierten und genutzten Produkten und Applikationen gefährden. Um vor der Migration die nötigen Überprüfungen zu ermöglichen, wird ITS, sofern verlangt und/oder notwendig, die Kontaktdaten der technischen Ansprechpartner der Unternehmen zur Verfügung stellen, die die auf den Systemen installierten Applikationen vertreiben oder warten. Etwaige Ausfälle mangels Kompatibilität von Applikationen mit neuen Systemen haben Vertragsstrafen zur Folge.

Der Zuschlagsempfänger kann auf den Systemen von ITS gegebenenfalls Produkte installieren, die für die Durchführung der Migration notwendig sind, muss jedoch garantieren, dass diese Produkte nicht die ordnungsgemäße Funktion der Systeme und Software in der Produktion beeinträchtigen und keine Konflikte mit der Produktions-Infrastruktur des aktuellen Dienstleisters verursachen, insbesondere hinsichtlich der Datensicherung. Soweit für die Durchführung der Migration nötig, kann auf der aktuellen Infrastruktur in dem Netz, in dem sich auch die Produktionssysteme befinden, ein virtueller Server erstellt werden. Die von ITS getragenen Kosten für die Einrichtung und Wartung dieses Servers auf der aktuellen Infrastruktur, einschließlich etwaiger Lizenzgebühren, werden vom Zuschlagsempfänger in Form professioneller Dienstleistungen im Wert ihres Gesamtbetrags zurückerstattet. Der Zuschlagsempfänger kann sich jedoch aus offenkundigen Sicherheitsgründen nicht direkt mit dem Virtualisierungssystem und/oder dem Backup-System des aktuellen Dienstleisters verbinden.

Die Netzwerkadressen der Niederlassungen von ITS dürfen durch die Migration nicht geändert werden; der aktuelle IP-Adressenplan bleibt unverändert. Die IP-Adressen der Systeme im Rechenzentrum sollten ebenfalls möglichst nur geändert werden, wenn dies aus technischen Gründen zwingend erforderlich ist. Bei einer Änderung der IP-Adressen der Systeme im Rechenzentrum obliegt es dem Zuschlagsempfänger, für die Änderung der Konfiguration der Server, Applikationen, Clients und etwaiger Netzgeräte Sorge zu tragen, die zur korrekten Durchführung der Änderung des Adressenplans notwendig sind, ohne dass dadurch in der Migrationsphase größere Belastungen für ITS entstehen oder die Benutzer in ihrer Arbeit eingeschränkt werden.

Was die aktuell vorhandenen Netzverbindungen betrifft, muss der Zuschlagsempfänger im Projektplan alle erforderlichen Arbeiten der aktuellen Netzbetreiber aufführen und einen Plan der Konfigurationen, die für die Durchführung der Migration nötig sind. Die Kosten für die Neukonfiguration vorhandener Geräte gehen zulasten des Auftraggebers. Soweit es notwendig ist, im Rechenzentrum des Zuschlagsempfängers neue Leitungen zu legen, trägt der Zuschlagsempfänger die dafür anfallenden Kosten.

Auf keinen Fall dürfen sich aus den Arbeiten zur Migration Probleme für die Infrastruktur des aktuellen Dienstleisters ergeben. Etwaige vom aktuellen Dienstleister geltend gemachte Schäden, die auf die Migration zurückzuführen sind, gehen vollumfänglich zulasten des Zuschlagsempfängers.
Der Zuschlagsempfänger ist befugt, wenn dies nach seiner Ansicht die Migration der Systeme erleichtert, sich eigenständig mit dem aktuellen Dienstleister über den Bezug nicht in diesem Leistungsverzeichnis beschriebener Dienstleistungen (zum Beispiel die Bereitstellung einer direkten Verbindung mit den Virtualisierungssystemen des Dienstleisters oder die Installation eigener Geräte im Rechenzentrum des aktuellen Dienstleisters usw.) zu einigen, sofern er die Kosten für diese Dienstleistungen übernimmt und aus derartigen Vereinbarungen keine größeren Belastungen für den Auftraggeber resultieren.
Die Migration gilt mit der Abnahme der vorgeschlagenen Infrastruktur als abgeschlossen. Bei der Abnahme, die der Zuschlagsempfänger und zuständige Mitarbeiter von ITS gemeinsam vornehmen, wird die vollständige Übereinstimmung der Lösungen mit den Anforderungen dieses Leistungsverzeichnisses überprüft.

2.19. Organisation des Dienstes nach der Migration

Der Zuschlagsempfänger muss im Anschluss an die Abnahme nach der Migration gemäß dem technischen Angebot und den Anforderungen dieses Leistungsverzeichnisses den Dienst aufnehmen.
Zur Leistung des Dienstes muss der Zuschlagsempfänger ITS die folgenden organisatorischen Werkzeuge bereitstellen:

- ein Trouble Ticketing-System, das jede Anfrage eindeutig identifiziert und Folgendes aufzeichnet:
  - Datum und Uhrzeit der Meldung;
  - Datum und Uhrzeit der Aufnahme der Anfrage und Bezeichnung des Technikers, der sie bearbeitet;
  - Datum und Uhrzeit der Behebung des Störfalls;
  - Zuordnung der Priorität und Schwere der Anfrage;
  - etwaige Eskalationen auf Anweisung von ITS oder automatisch in Abhängigkeit von der Einhaltung der SLA (Service Level Agreement) gemäß Kapitel **Errore. L'origine riferimento non è stata trovata.**;
  - Beschreibung der Phasen der Bearbeitung und Lösung etwaiger Probleme oder Störfälle.

  Das Trouble Ticketing-System muss für ITS über eine Web-Oberfläche zugänglich sein, die es erlaubt, neue Anfragen zu öffnen, den Status in Bearbeitung befindlicher Anfragen zu kontrollieren, bestehenden Anfragen Informationen oder Anforderungen hinzuzufügen, die Priorität von Anfragen zu ändern und/oder sie an ein höheres Support-Niveau zu eskalieren;
- eine Telefonnummer des Service Desk des Dienstleisters, die die Service-Ansprechpartner von ITS oder die Dienstbezieher selbst bei Problemen auf der ersten Ebene anrufen können. Nach dem Telefonanruf wird im Trouble Ticketing-System ein Ticket zur Verfolgung der Bearbeitung geöffnet, und der Gesprächspartner erhält die Identifikationsnummer seiner Anfrage;

- ein E-Mail-Postfach zur automatischen Öffnung einer Anfrage im Trouble Ticketing-System, das eingehende Mails unter Angabe der Identifikationsnummer des geöffneten Tickets beantwortet.

Der Service Desk muss während der Arbeitszeiten montags bis freitags zwischen 07:30 Uhr und 17:30 Uhr erreichbar und mit zweisprachigem Personal (italienisch und deutsch) besetzt sein, das die Anrufe in der vom Anrufer gewählten Sprache beantwortet. Der Service Desk muss seinen Dienst auf Wunsch des Anrufers auch in englischer Sprache erbringen können, da er eventuell mit externen Dienstleistern kommunizieren muss.
Zusätzlich zum Service Desk muss der Zuschlagsempfänger ITS die Nummer einer Rufbereitschaft zur Verfügung stellen, die außerhalb der Dienstzeiten des Service Desk erreichbar ist und direkt Support der zweiten Ebene leistet. Die Rufbereitschaft kann nur von Service-Ansprechpartnern von ITS (die bei Aufnahme ihres Dienstes bekanntgegeben werden) bei dringenden Problemen oder außerhalb der Arbeitszeiten genutzt werden. Die Kosten für eventuelle Arbeiten, die, veranlasst durch einen Anruf der Rufbereitschaft, außerhalb der Arbeitszeiten durchgeführt werden, werden den im Kapitel **Errore. L'origine riferimento non è stata trovata.** definierten Ressourcen belastet.
Außerdem hat der Zuschlagsempfänger unter seinen Mitarbeitern einen geschäftlichen und einen technischen Ansprechpartner zu benennen, die im Notfall oder bei einer notwendigen Eskalierung von Meldungen kontaktiert werden können. Der Zuschlagsempfänger muss die direkten Kontaktdaten der benannten Personen bei Abschluss des Vertrags mitteilen. Der Zugang zu diesen Ressourcen ist ausschließlich den Service-Ansprechpartnern von ITS vorbehalten, die ihrerseits dem Zuschlagsempfänger bekanntgegeben werden.

3. Time & Material

Der Zuschlagsempfänger muss über alle Arbeiten, die nicht mit der Servicegebühr abgegolten sind, ein Dienstleistungsangebot erstellen und hierzu die Formel „Stundenabrechnung“ für die folgenden Profile verwenden:

- Junior-Systemtechniker
- Senior-Systemtechniker.

Senior-Systemtechniker ist eine Fachkraft, die über eine mindestens fünfjährige Berufserfahrung in der betreffenden Technologie oder über eine dreijährige Berufserfahrung und eine Zertifizierung des Verkäufers des Produkts verfügt (sofern zutreffend).
Junior-Systemtechniker ist eine Fachkraft, die nicht über die Qualifikation eines Senior-Systemtechnikers verfügt.
Das Stundenkontingent, das für Fachkräfte dieser beiden Qualifikationsstufen jeweils getrennt festgelegt wird, beläuft sich für die gesamte Vertragslaufzeit auf 300 Stunden. ITS kann die technischen Ressourcen nach seinem Ermessen für alle Tätigkeiten nutzen, die nicht Gegenstand des Dienst- und Beratungsvertrags sind. Die für Fachkräfte der beiden Qualifikationsstufen vorgesehenen Stunden können unabhängig vom Tag und der Uhrzeit, zu der die angeforderte Arbeit ausgeführt werden muss, genutzt werden. Zuschläge für Arbeit an Feiertagen, an Tagen vor einem Feiertag oder während der Nacht werden nicht erhoben. Die geleisteten Arbeitsstunden werden nach angefangenen Zeiträumen von je 15 Minuten berechnet.

ITS kann, wenn es für den Dienst erforderlich ist, während der Vertragslaufzeit beim Zuschlagsempfänger beantragen, das verfügbare Arbeitsstundenkontingent um zusätzliche Fachkraftstunden beider oder einer der oben genannten Qualifikationsstufen zu erhöhen.
Sollte das Stundenkontingent bei Vertragsende nicht vollständig verbraucht sein, kann ITS die nicht verbrauchten Arbeitsstunden auf Antrag innerhalb von 3 Kalenderjahren nach Beendigung des Vertrags für Arbeiten nutzen, die keinen Bezug zu der Dienstleistung haben.

4. Dienstgütestufen

Der Zuschlagsempfänger muss eine wirksame Erbringung der Dienstleistungen garantieren und bei Problemen, je nach deren Schwere und Priorität, die nachstehend aufgeführten Dienstgütestufen einhalten. Zur Kontrolle der Dienstgütestufen hat der Dienstleister einen monatlichen Bericht auf Basis der vom im Kapitel **Errore. L'origine riferimento non è stata trovata.** beschriebenen Trouble Ticketing-System erfassten Daten vorzulegen, der eine Übersicht über alle im Berichtsmonat von ITS und seinen Benutzern getätigten Anrufe enthält, unter Angabe von Datum und Zeit des Gesprächsbeginns, der Aufnahme der Anfrage und des Abschlusses des Telefongesprächs, der der Anfrage zugewiesenen Schwere und Priorität, der Bezeichnung des aufnehmenden Technikers und des Gegenstand des Anrufs.
Welche Schwere und Priorität einem Problem zuzuweisen ist, ergibt sich aus folgender Tabelle:

Schwere	**Beschreibung**	**Aufnahme des Störfalls**	**Behebung des Störfalls**
Hoch	Probleme, die die Unterbrechung eines Dienstes verursachen, die alle Benutzer einer oder mehrerer Niederlassungen von ITS oder mindestens eine geschäftskritische Applikation betrifft.	innerhalb von 2 Zeitstunden	innerhalb von 24 Zeitstunden
Mittel	Probleme, die eine Unterbrechung von Diensten verursachen, die eine geringere Anzahl von Benutzern betrifft, oder die partielle Ausfälle, jedoch keine Betriebsunterbrechung, verursachen (z. B. Leistungsverminderung, Aktivierung redundanter Hardware usw.)	innerhalb von 4 Arbeitsstunden	innerhalb von 16 Arbeitsstunden
Niedrig	Probleme, die keine Ausfälle bei den Nutzern des IT-Systems verursachen (z. B. Warnungen der Backup-Software usw.)	innerhalb von 8 Arbeitsstunden	innerhalb von 24 Arbeitsstunden
Null	Informationsanfrage oder Support bei Problemen, die keinen Ausfall verursachen	innerhalb von 8 Arbeitsstunden	innerhalb von 40 Arbeitsstunden

Die Zeitangaben in der Spalte „Aufnahme des Störfalls“ beziehen sich auf den Zeitraum zwischen dem Beginn des Telefongesprächs mit dem Service Desk oder der Rufbereitschaft und den ersten Maßnahmen des beauftragten Technikers zur Diagnose und Lösung des Problems, die per E-Mail dem Benutzer mitzuteilen sind, der die Meldung mit der Öffnung des Tickets erstattet hat.

Die Zeitangaben in der Spalte „Behebung des Störfalls“ beziehen sich auf den Zeitraum zwischen dem Beginn des Telefongesprächs mit dem Service Desk oder der Rufbereitschaft und der Lösung des gemeldeten Problems oder der Herabstufung seiner Schwere, zum Beispiel durch eine Notlösung, die es erlaubt, den Dienst teilweise wieder aufzunehmen, oder eine vorläufige Lösung, die später zu überprüfen ist.
Die Nichteinhaltung des SLA (Service Level Agreement) begründet gemäß dem Vertrag die Verhängung von Vertragsstrafen.

5. Erweiterungen

Zurzeit ist keine erhebliche Erweiterung des ausgeschriebenen Leistungsumfangs während der Vertragslaufzeit vorgesehen. Die einzigen bereits vorgesehenen und in den vorstehenden Kapiteln erwähnten Arbeiten sind die Verlagerung der Applikation SAP von Brixen in das Rechenzentrum, die vor Abschluss des Vertrags voraussichtlich abgeschlossen ist, und die Inbetriebnahme der neuen Niederlassung in der Albertina-Brogliati-Straße in Meran im ersten Jahr nach Aufnahme des Dienstes. Gleichwohl können künftige Entwicklungen dazu führen, dass neue virtuelle Server oder neue virtuelle Arbeitsplätze bereitgestellt werden müssen sowie neue Niederlassungen und weitere Benutzer der bestehenden Infrastruktur hinzukommen. Der Zuschlagsempfänger verpflichtet sich, ITS und seinen Teilhabern die nötigen Ressourcen für eventuelle Änderungen zur Verfügung zu stellen, die sich während der Vertragslaufzeit eventuell abzeichnen.
Bitte beachten Sie, dass im Falle von Unstimmigkeiten/Unvollständigkeiten in den technischen Spezifikationen in deutscher Sprache auf die technischen Spezifikationen in italienischer Sprache verwiesen werden sollte.