UGT მომსახურების დონის ხელშეკრულება (SLA)

ვერსია: 1.1
ძალაში შესვლის თარიღი: [12 აგვისტო, 2021]
ბოლო გადახედვის თარიღი: [10 აპრილი, 2025]

1. შესავალი

წინამებარე მომსახურების დონის ხელშეკრულება ("SLA") განსაზღვრავს მომსახურების სტანდარტებს, მხარდაჭერის ვალდებულებებს, პასუხისმგებლობებს, ესკალაციის პროცედურებსა და შესრულების მიზნებს, რომლებიც ვრცელდება UGT-ის ("მიმწოდებელი") მიერ მისი კლიენტებისთვის ("კლიენტი") მიწოდებულ მომსახურებებზე.
ამ SLA-ის მიზანია ჩამოაყალიბოს მკაფიო მოლოდინები მიმწოდებლისგან შეძენილი Microsoft-ის ღრუბლოვანი სერვისებისა და მათთან დაკავშირებული მართვადი სერვისების მხარდაჭერასთან, ადმინისტრირებასთან, მართვასა და ტექნიკურ მომსახურებასთან დაკავშირებით.
წინამდებარე დოკუმენტი მიზნად ისახავს გამჭვირვალობის, ანგარიშვალდებულებისა და ეფექტური კომუნიკაციის ხელშეწყობას მიმწოდებელსა და კლიენტს შორის, რათა უზრუნველყოფილ იქნას ინციდენტების, მოთხოვნებისა და მომსახურებასთან დაკავშირებული საკითხების თანმიმდევრული და პროფესიონალური გადაწყვეტა.
ეს SLA წარმოადგენს მიმწოდებელსა და კლიენტს შორის სახელშეკრულებო ურთიერთობის ნაწილს და უნდა განიხილებოდეს მხარეებს შორის გაფორმებულ მომსახურების ძირითად ხელშეკრულებასთან (MSA), მართვადი მომსახურების ხელშეკრულებასთან, გამოწერის ხელშეკრულებასთან, სამუშაოს აღწერილობასთან (SOW) ან შეკვეთის ფორმასთან ერთობლიობაში.

2. მომსახურების სფერო

მიმწოდებელი უზრუნველყოფს ღრუბლოვან ლიცენზირებას, ტექნიკურ მხარდაჭერასა და მართვად სერვისებს Microsoft-ის ტექნოლოგიებთან და მასთან დაკავშირებულ გადაწყვეტილებებთან მიმართებაში.
ამ SLA-ით გათვალისწინებული სერვისები შეიძლება მოიცავდეს შემდეგს:
Microsoft-ის ღრუბლოვანი სერვისები

- Microsoft 365
- Office 365
- Microsoft Azure
- Dynamics 365
- Microsoft Teams
- Exchange Online
- SharePoint Online
- OneDrive for Business
- Power Platform
- Microsoft Defender
- Microsoft Intune
- Microsoft Entra ID

პროფესიონალური და მართვადი სერვისები

- ლიცენზიების შესყიდვა და ადმინისტრირება
- მომხმარებლის ანგარიშების მართვა
- ტენანტის (Tenant) ადმინისტრირება

- უსაფრთხოების პოლიტიკის კონფიგურაცია
- ტექნიკური მხარდაჭერა და ხარვეზების აღმოფხვრა
- ინციდენტების მართვა
- ცვლილებების მართვა
- მომსახურების მოთხოვნების შესრულება
- მხარდაჭერის ესკალაცია Microsoft-თან
- გამოწერების (Subscriptions) მართვა
- რეპორტინგი და საკონსულტაციო მომსახურება

კლიენტისთვის გაწეული კონკრეტული სერვისები განისაზღვრება კლიენტის მიერ შეძენილი მომსახურების პაკეტის ან გამოწერის მიხედვით.

3. მომსახურების ხელმისაწვდომობა

3.1 Microsoft-ის ღრუბლოვანი სერვისები

Microsoft ფლობს და მართავს ინფრასტრუქტურას, რომელიც უზრუნველყოფს Microsoft-ის ღრუბლოვან სერვისებს. Microsoft-ის მიერ ჰოსტირებული სერვისების ხელმისაწვდომობის ვალდებულებები რეგულირდება Microsoft-ის ოფიციალური მომსახურების დონის ხელშეკრულებებითა და მომსახურების პირობებით.
მიმწოდებელი დამოუკიდებლად ვერ იძლევა Microsoft-ის გლობალური ღრუბლოვანი ინფრასტრუქტურის ხელმისაწვდომობის, უწყვეტი მუშაობის (uptime), წარმადობის ან ფუნქციონირების გარანტიას. მაგალითები მოიცავს:

- Microsoft 365
- Azure
- Exchange Online
- SharePoint Online
- Teams
- Dynamics 365
- Power Platform

ნებისმიერი შეფერხება, რომელიც სათავეს იღებს Microsoft-ის ინფრასტრუქტურიდან, დაექვემდებარება Microsoft-ის მომსახურების მართვის პროცესებსა და ხარვეზების აღმოფხვრის ვადებს. საჭიროების შემთხვევაში, მიმწოდებელი დაეხმარება კლიენტს Microsoft-თან მხარდაჭერის ქეისების (cases) გახსნაში, მართვასა და ესკალაციაში.

3.2 მიმწოდებლის მხარდაჭერის სერვისები

მიმწოდებელი გამოიყენებს კომერციულად გონივრულ ძალისხმევას, რათა უზრუნველყოს მხარდაჭერის სერვისების ხელმისაწვდომობა ქვემოთ განსაზღვრული სამუშაო საათების შესაბამისად:

მომსახურება	**ხელმისაწვდომობა**
საინფორმაციო/მხარდაჭერის მაგიდა (Helpdesk)	ორშაბათი-პარასკევი, 10:00-18:00
ელ.ფოსტით მხარდაჭერა	მოთხოვნის გაგზავნა 24x7 რეჟიმში
გადაუდებელი მხარდაჭერა	24x7 კრიტიკული ინციდენტებისთვის

კლიენტების მართვა (Account Management)	სამუშაო საათები

სამუშაო საათები განისაზღვრება ორშაბათიდან პარასკევის ჩათვლით, მიმწოდებლის მიერ ოფიციალურად გამოცხადებული უქმე დღეების გამოკლებით.

4. ინციდენტების მართვა

ინციდენტი განისაზღვრება, როგორც IT მომსახურების ხარისხის ნებისმიერი დაუგეგმავი შეწყვეტა, გაუარესება ან შემცირება.
კლიენტის მიერ მოხსენებული ყველა ინციდენტი შეფასდება და მიენიჭება პრიორიტეტის დონე ბიზნესზე გავლენისა და გადაუდებლობის საფუძველზე. მიმწოდებელი იტოვებს უფლებას, მოკვლევის შემდეგ, საჭიროებისამებრ შეცვალოს ინციდენტის პრიორიტეტი.

5. ინციდენტების პრიორიტეტების კლასიფიკაცია

პრიორიტეტი 1 – კრიტიკული ინციდენტი (Critical)
კრიტიკულია ინციდენტი, რომელიც იწვევს არსებითი ბიზნეს ოპერაციების სრულ შეფერხებას და ხელს უშლის მომხმარებელთა მნიშვნელოვან რაოდენობას კრიტიკული ბიზნეს ფუნქციების შესრულებაში.
მაგალითები:

- Microsoft 365-ის სრული გათიშვა, რომელიც გავლენას ახდენს ორგანიზაციაზე
- ელექტრონული ფოსტის გათიშვა ორგანიზაციის მასშტაბით
- უსაფრთხოების დარღვევა ან აქტიური კიბერინციდენტი
- ტენანტზე (Tenant) წვდომის შეუძლებლობა
- Azure-ის საწარმოო (production) გარემოს მიუწვდომლობა

მომსახურების ვალდებულება:

- პირველადი რეაგირება: 2 საათის განმავლობაში
- ესკალაცია: დაუყოვნებლივ
- სტატუსის განახლება: ყოველ 4 საათში ერთხელ
- მხარდაჭერის დაფარვა: 24x7

პრიორიტეტი 2 – მაღალი ინციდენტი (High)
მაღალი პრიორიტეტის ინციდენტი მნიშვნელოვნად აფერხებს ბიზნეს ოპერაციებს, მაგრამ არ იწვევს სრულ გათიშვას.
მაგალითები:

- რამდენიმე მომხმარებელი ვერ ახერხებს სერვისებზე წვდომას
- Teams-ის ძირითადი ფუნქციონალის ხარვეზი
- ავტორიზაციის ხარვეზები, რომლებიც გავლენას ახდენს კონკრეტულ დეპარტამენტებზე
- აპლიკაციის წარმადობის მნიშვნელოვანი გაუარესება

მომსახურების ვალდებულება:

- პირველადი რეაგირება: 4 საათის განმავლობაში
- სტატუსის განახლება: ყოველ 6 საათში ერთხელ
- ესკალაცია: საჭიროებისამებრ

პრიორიტეტი 3 – საშუალო ინციდენტი (Medium)
საშუალო პრიორიტეტის ინციდენტი გავლენას ახდენს ცალკეულ მომხმარებლებზე ან არაკრიტიკულ ბიზნეს პროცესებზე, რომელთათვისაც არსებობს ალტერნატიული გზები (workarounds).
მაგალითები:

- მომხმარებლის საფოსტო ყუთის პრობლემები
- ერთი მომხმარებლის ავტორიზაციის პრობლემა

- ლიცენზიის მინიჭების პრობლემები
- კონფიგურაციასთან დაკავშირებული ხარვეზები

მომსახურების ვალდებულება:

- პირველადი რეაგირება: 8 სამუშაო საათის განმავლობაში
- სტატუსის განახლება: ყოველდღიურად

პრიორიტეტი 4 – დაბალი ინციდენტი (Low)

დაბალი პრიორიტეტის ინციდენტები მოიცავს რუტინულ მოთხოვნებს, საინფორმაციო შეკითხვებს და მცირე საკითხებს, რომლებსაც ნაკლებად აქვთ ან საერთოდ არ აქვთ გავლენა ბიზნესზე.

მაგალითები:

- ზოგადი დახმარების მოთხოვნები
- ახალი მომხმარებლის დამატების (onboarding) მოთხოვნები
- რეპორტინგის მოთხოვნები
- საკონსულტაციო შეხვედრები

მომსახურების ვალდებულება:

- პირველადი რეაგირება: 1 სამუშაო დღის განმავლობაში
- განახლებები: საჭიროებისამებრ

6. მომსახურების მოთხოვნების მართვა

მომსახურების მოთხოვნები (Service Requests) არის სტანდარტული ოპერაციული მოთხოვნები, რომლებიც არ არის გამოწვეული სერვისის გაუმართაობით.

მაგალითები:

- ახალი მომხმარებლის შექმნა
- ლიცენზიის მინიჭება
- საერთო საფოსტო ყუთის (Shared mailbox) შექმნა
- სადისტრიბუციო ჯგუფების ცვლილებები
- პაროლის აღდგენა
- მოწყობილობის რეგისტრაცია (enrollment)
- უსაფრთხოების პოლიტიკის განახლება

მიმწოდებელი გამოიყენებს გონივრულ ძალისხმევას მოთხოვნების შესასრულებლად შემდეგ ვადებში:

მოთხოვნის ტიპი	**შესრულების მიზნობრივი ვადა**
პაროლის აღდგენა	4 საათი
მომხმარებლის შექმნა	1 სამუშაო დღე
ლიცენზიის მინიჭება	4 სამუშაო საათი
საფოსტო ყუთის შექმნა	1 სამუშაო დღე
უსაფრთხოების ჯგუფის ცვლილებები	1 სამუშაო დღე
გამოწერის (Subscription) ცვლილებები	2 სამუშაო დღე
სტანდარტული კონფიგურაციის ცვლილებები	3 სამუშაო დღე

შენიშვნა: შესრულების მიზნობრივი ვადები წარმოადგენს ორიენტირს და არ არის ხარვეზის აღმოფხვრის გარანტირებული დრო.

7. ესკალაციის პროცედურები

მიმწოდებელი ინარჩუნებს ესკალაციის სტრუქტურირებულ პროცესს ინციდენტების ეფექტური გადაწყვეტის უზრუნველსაყოფად.

- **დონე 1 – საინფორმაციო/მხარდაჭერის მაგიდა (Service Desk):** პირველი ხაზის მხარდაჭერა, რომელიც პასუხისმგებელია პირველად დიაგნოსტიკაზე, ტრიაჟსა და გავრცელებული პრობლემების მოგვარებაზე.
- **დონე 2 – ტექნიკური სპეციალისტები:** პასუხისმგებელნი არიან სიღრმისეულ პრობლემების აღმოფხვრასა და ხარვეზების გამოსწორებაზე.
- **დონე 3 – ვენდორთან ესკალაცია:** საკითხები, რომლებიც გამოწვეულია Microsoft-ის სერვისების შიდა ხარვეზით, შეიძლება ესკალირებულ იქნას Microsoft-ის მხარდაჭერის გუნდთან. Microsoft-თან დაკავშირებული პრობლემების გადაჭრის ვადები დამოკიდებულია Microsoft-ის შიდა მხარდაჭერის პროცედურებზე და მიმწოდებელი მათზე გარანტიას ვერ გასცემს.

8. კლიენტის პასუხისმგებლობები

მომსახურების წარმატებით მიწოდების უზრუნველსაყოფად, კლიენტი თანახმაა:

- მიაწოდოს ზუსტი ინფორმაცია ინციდენტების მოხსენებისას.
- დანიშნოს უფლებამოსილი საკონტაქტო პირები მხარდაჭერისთვის.
- შეინარჩუნოს მოქმედი ლიცენზიები და გამოწერები.
- ითანამშრომლოს ხარვეზების აღმოფხვრის პროცესში.
- უზრუნველყოს საბოლოო მომხმარებლების მიერ ორგანიზაციული პოლიტიკის დაცვა.
- შეინარჩუნოს უსაფრთხოების სათანადო კონტროლი კლიენტის მფლობელობაში არსებულ სისტემებზე.
- დაუყოვნებლივ შეატყობინოს მიმწოდებელს ბიზნესზე გავლენის მქონე ცვლილებების შესახებ.
- განაახლოს მიმდინარე საკონტაქტო ინფორმაცია.

ამ პასუხისმგებლობების შეუსრულებლობამ შესაძლოა გავლენა იქონიოს მიმწოდებლის შესაძლებლობაზე, შეასრულოს მომსახურების მიზნობრივი ვადები.

9. უსაფრთხოება და შესაბამისობა

მიმწოდებელი აცნობიერებს კლიენტის მონაცემების დაცვისა და უსაფრთხო მომსახურების პრაქტიკის შენარჩუნების მნიშვნელობას.

მიმწოდებელი ვალდებულია:

- შეინარჩუნოს უსაფრთხო ადმინისტრაციული პროცედურები.
- გამოიყენოს მრავალფაქტორიანი ავტორიზაცია (MFA) პრივილეგირებული წვდომისთვის.
- მიჰყვეს ინდუსტრიის სტანდარტების შესაბამის კიბერუსაფრთხოების პრაქტიკას.
- შეზღუდოს წვდომა მხოლოდ უფლებამოსილ პერსონალზე.
- დაიცვას კლიენტის ინფორმაციის კონფიდენციალურობა.
- შეატყობინოს კლიენტებს დადასტურებული უსაფრთხოების ინციდენტების შესახებ, რომლებიც გავლენას ახდენენ მართვის ქვეშ მყოფ სერვისებზე.

მიმწოდებელი არ იძლევა ყველა კიბერუსაფრთხოების საფრთხის, თავდასხმის ან უნებართვო წვდომის პრევენციის აბსოლუტურ გარანტიას.

10. დაგეგმილი ტექნიკური სამუშაოები

მიმწოდებელმა შეიძლება პერიოდულად ჩაატაროს ტექნიკური სამუშაოები, რომლებიც აუცილებელია მომსახურების ხარისხის, უსაფრთხოებისა და ოპერაციული სტაბილურობის შესანარჩუნებლად.

ყოველი გონივრული შესაძლებლობის ფარგლებში, კლიენტები წინასწარ მიიღებენ შეტყობინებას დაგეგმილი ტექნიკური სამუშაოების შესახებ. ტექნიკური სამუშაოები შეიძლება მოიცავდეს:

- უსაფრთხოების განახლებებს
- პლატფორმის განახლებებს (upgrades)
- ინფრასტრუქტურის გაუმჯობესებას
- სერვისის ოპტიმიზაციას
- კონფიგურაციის ცვლილებებს

გადაუდებელი ტექნიკური სამუშაოები შეიძლება ჩატარდეს წინასწარი შეტყობინების გარეშე, როდესაც ეს აუცილებელია მომსახურების მთლიანობის ან უსაფრთხოების დასაცავად.

11. გამონაკლისები

ეს SLA არ ვრცელდება მომსახურების შეფერხებებზე, რომლებიც გამოწვეულია:

- Microsoft-ის გლობალური სერვისების გათიშვით
- ინტერნეტ პროვაიდერის ხარვეზებით
- კლიენტის მფლობელობაში არსებული აპარატურის გაუმართაობით
- კლიენტის ქსელის გაუმართაობით
- კლიენტის მხარეს არასწორი კონფიგურაციით
- მესამე მხარის მიერ განხორციელებული უნებართვო ცვლილებებით
- ფორსმაჟორული გარემოებებით
- ბუნებრივი კატასტროფებით
- სამთავრობო ქმედებებით
- ელექტროენერგიის გათიშვით მიმწოდებლის კონტროლს მიღმა
- კლიენტის დაუდევრობით გამოწვეული კიბერუსაფრთხოების ინციდენტებით
- მხარდაჭერის არმქონე პროგრამული უზრუნველყოფით ან სისტემებით

მიმწოდებელი არ არის პასუხისმგებელი შეფერხებებზე, რომლებიც გამოწვეულია მის გონივრულ კონტროლს მიღმა არსებული გარემოებებით.

12. რეპორტინგი და მომსახურების გადახედვა

მიმწოდებელმა შეიძლება ჩაატაროს მომსახურების პერიოდული გადახედვა, რათა შეაფასოს სერვისის ეფექტურობა, გამოავლინოს გაუმჯობესების შესაძლებლობები და განიხილოს ოპერაციული საკითხები.

გადახედვა შეიძლება მოიცავდეს:

- ინციდენტების ტენდენციებს
- მომსახურების ეფექტურობის მეტრიკას
- უსაფრთხოების რეკომენდაციებს
- ლიცენზირების ოპტიმიზაციას
- სტრატეგიულ ტექნოლოგიურ დაგეგმვას

13. პასუხისმგებლობის შეზღუდვა

მიმწოდებლის ვალდებულებები ამ SLA-ის ფარგლებში შემოიფარგლება მხოლოდ აქ მკაფიოდ აღწერილი მხარდაჭერისა და მართვადი სერვისებით.

მიმწოდებელი არ არის პასუხისმგებელი არაპირდაპირ, შემთხვევით, სპეციალურ, შედეგობრივ ან საჯარიმო ზიანზე, რომელიც გამოწვეულია მომსახურების შეწყვეტით, მონაცემთა დაკარგვით, ბიზნესის შეფერხებით ან მოგების დაკარგვით. პასუხისმგებლობა ექვემდებარება მხარეებს შორის გაფორმებულ ძირითად სახელშეკრულებო შეთანხმებაში განსაზღვრულ შეზღუდვებს.

14. SLA-ის გადახედვა და ცვლილებები

ეს SLA შეიძლება პერიოდულად გადაიხედოს ოპერაციული ცვლილებების, მომსახურების გაუმჯობესების, მარეგულირებელი მოთხოვნების ან ბიზნეს საჭიროებების ასახვის მიზნით. მიმწოდებელი იტოვებს უფლებას შეცვალოს ეს SLA კლიენტის გონივრული წერილობითი შეტყობინების საფუძველზე. უახლესი ვერსია ანაცვლებს ყველა წინა ვერსიას.

16. საკონტაქტო ინფორმაცია

საინფორმაციო/მხარდაჭერის მაგიდა (Service Desk)
ელ.ფოსტა: Helpdesk@ugt.ge
ტელეფონი: +995 32 2220505
მხარდაჭერის საათები: ორშაბათი-პარასკევი, 10:00-18:00

თანხმობა

UGT-ის მიერ მიწოდებული სერვისების შეძენით, გამოწერით ან გამოყენებით, კლიენტი ადასტურებს, რომ წაიკითხა, გაიგო და დაეთანხმა წინამებარე მომსახურების დონის ხელშეკრულებაში მოცემულ პირობებსა და წესებს.

UGT SERVICE LEVEL AGREEMENT (SLA)

Version: 1.1
Effective Date: [August 12, 2021]
Last Review Date: [April 10, 2025]

1. Introduction

This Service Level Agreement ("SLA") defines the service standards, support commitments, responsibilities, escalation procedures, and performance objectives applicable to services delivered by **UGT** ("Provider") to its customers ("Customer").
The purpose of this SLA is to establish clear expectations regarding the support, administration, management, and maintenance of Microsoft cloud services and associated managed services purchased through the Provider.
This document is intended to promote transparency, accountability, and effective communication between the Provider and the Customer, ensuring that incidents, requests, and service-related matters are addressed in a consistent and professional manner.
This SLA forms part of the contractual relationship between the Provider and the Customer and should be read in conjunction with any Master Services Agreement (MSA), Managed Services Agreement, Subscription Agreement, Statement of Work (SOW), or Order Form executed between the parties.

2. Scope of Services

The Provider delivers cloud licensing, technical support, and managed services associated with Microsoft technologies and related solutions.
Services covered under this SLA may include:

Microsoft Cloud Services

- Microsoft 365
- Office 365
- Microsoft Azure
- Dynamics 365
- Microsoft Teams
- Exchange Online
- SharePoint Online
- OneDrive for Business
- Power Platform
- Microsoft Defender
- Microsoft Intune
- Microsoft Entra ID

Professional and Managed Services

- License procurement and administration
- User account management
- Tenant administration
- Security policy configuration
- Technical support and troubleshooting
- Incident management

- Change management
- Service request fulfillment
- Microsoft support escalation
- Subscription management
- Reporting and advisory services

The specific services provided to the Customer shall be determined by the service package or subscription purchased by the Customer.

3. Service Availability

3.1 Microsoft Cloud Services

Microsoft owns and operates the infrastructure supporting Microsoft cloud services. Availability commitments for Microsoft-hosted services are governed by Microsoft's official service level agreements and service terms.

The Provider does not independently guarantee the availability, uptime, performance, or functionality of Microsoft's global cloud infrastructure.

Examples include:

- Microsoft 365
- Azure
- Exchange Online
- SharePoint Online
- Teams
- Dynamics 365
- Power Platform

Any service interruption originating within Microsoft's infrastructure shall be subject to Microsoft's service management processes and remediation timelines.

Where applicable, the Provider will assist the Customer by opening, managing, and escalating support cases with Microsoft.

3.2 Provider Support Services

The Provider shall make commercially reasonable efforts to ensure the availability of support services according to the service coverage defined below.

Service	Availability
Helpdesk Support	Monday-Friday, 10:00-18:00
Email Support	24x7 Submission
Emergency Support	24x7 for Critical Incidents
Account Management	Business Hours

Business Hours are defined as Monday through Friday, excluding public holidays observed by the Provider.

4. Incident Management

An incident is defined as any unplanned interruption, degradation, or reduction in quality of an IT service.

All incidents reported by the Customer will be assessed and assigned a priority level based on business impact and urgency.

The Provider reserves the right to adjust incident priority where appropriate after investigation.

5. Incident Priority Classification

Priority 1 – Critical Incident

A Critical Incident is one that causes a complete disruption to essential business operations and prevents a significant number of users from performing critical business functions.

Examples include:

- Complete Microsoft 365 outage affecting the organization
- Organization-wide email failure
- Security breach or active cyber incident
- Tenant access unavailable
- Azure production environment unavailable

Service Commitment

- Initial Response: Within 2 Hour
- Escalation: Immediate
- Status Updates: Every 4 Hours
- Support Coverage: 24x7

Priority 2 – High Incident

A High Incident significantly affects business operations but does not result in a complete outage.

Examples include:

- Multiple users unable to access services
- Major Teams functionality failure
- Authentication failures affecting departments
- Significant application performance degradation

Service Commitment

- Initial Response: Within 4 Hours
- Status Updates: Every 6 Hours
- Escalation: As Required

Priority 3 – Medium Incident

A Medium Incident affects individual users or non-critical business processes with available workarounds.

Examples include:

- User mailbox issues
- Single-user login problems
- License assignment issues
- Configuration-related problems

Service Commitment

- Initial Response: Within 8 Business Hours
- Status Updates: Daily

Priority 4 – Low Incident

Low-priority incidents include routine requests, informational inquiries, and minor issues with little or no business impact.

Examples include:

- General assistance requests
- User onboarding requests
- Reporting requests
- Advisory consultations

Service Commitment

- Initial Response: Within 1 Business Day
- Updates: As Necessary

6. Service Request Management

Service Requests are standard operational requests that do not result from service failure.

Examples include:

- New user creation
- License assignment
- Shared mailbox creation
- Distribution group modifications
- Password resets
- Device enrollment
- Security policy updates

The Provider will use reasonable efforts to complete requests within the following target timeframes:

Request Type	Target Completion
Password Reset	4 Hour
User Creation	1 Business Day
License Assignment	4 Business Hours
Mailbox Creation	1 Business Day
Security Group Changes	1 Business Day
Subscription Changes	2 Business Days
Standard Configuration Changes	3 Business Days

Completion targets are objectives and not guaranteed resolution times.

7. Escalation Procedures

The Provider maintains a structured escalation process to ensure efficient resolution of incidents.

Level 1 – Service Desk

First-line support responsible for initial diagnosis, triage, and resolution of common issues.

Level 2 – Technical Specialists

Responsible for advanced troubleshooting and issue remediation.

Level 3 – Vendor Escalation

Issues determined to originate within Microsoft services may be escalated to Microsoft Support. Resolution timeframes for Microsoft-related issues remain dependent on Microsoft's internal support procedures and cannot be guaranteed by the Provider.

8. Customer Responsibilities

To ensure successful service delivery, the Customer agrees to:

- Provide accurate information when reporting incidents.
- Designate authorized support contacts.
- Maintain valid licensing and subscriptions.
- Cooperate with troubleshooting activities.
- Ensure end-user compliance with organizational policies.
- Maintain appropriate security controls on customer-owned systems.
- Promptly communicate business-impacting changes.

- Maintain current contact information.

Failure to meet these responsibilities may affect the Provider's ability to meet service targets.

9. Security and Compliance

The Provider recognizes the importance of protecting Customer data and maintaining secure service delivery practices.

The Provider shall:

- Maintain secure administrative procedures.
- Enforce multi-factor authentication for privileged access.
- Follow industry-standard cybersecurity practices.
- Restrict access to authorized personnel.
- Maintain confidentiality of Customer information.
- Notify Customers of verified security incidents impacting services under management.

The Provider does not guarantee prevention of all cybersecurity threats, attacks, or unauthorized access events.

10. Scheduled Maintenance

The Provider may periodically perform maintenance activities required to maintain service quality, security, and operational stability.

Whenever reasonably possible, Customers shall receive advance notice of planned maintenance activities.

Maintenance activities may include:

- Security updates
- Platform upgrades
- Infrastructure improvements
- Service optimization
- Configuration changes

Emergency maintenance may be performed without prior notification where necessary to protect service integrity or security.

11. Service Exclusions

This SLA does not apply to service interruptions resulting from:

- Microsoft global service outages
- Internet service provider failures
- Customer-owned hardware failures
- Customer network failures
- Customer misconfiguration
- Unauthorized third-party modifications
- Force majeure events
- Natural disasters
- Government actions
- Power failures outside Provider control
- Cybersecurity incidents caused by Customer negligence
- Unsupported software or systems

The Provider shall not be held liable for failures caused by circumstances beyond its reasonable control.

12. Reporting and Service Reviews

The Provider may conduct periodic service reviews to evaluate service performance, identify improvement opportunities, and discuss operational concerns.

Reviews may include:

- Incident trends
- Service performance metrics
- Security recommendations
- Licensing optimization
- Strategic technology planning

13. Limitation of Liability

The Provider's obligations under this SLA are limited to the support and managed services explicitly described herein.

The Provider shall not be liable for indirect, incidental, special, consequential, or punitive damages arising from service interruptions, data loss, business interruption, or loss of profits.

Liability shall remain subject to the limitations defined in the governing contractual agreement between the parties.

14. SLA Review and Amendments

This SLA may be reviewed periodically to reflect operational changes, service improvements, regulatory requirements, or business needs.

The Provider reserves the right to modify this SLA upon reasonable written notice to the Customer. The latest version shall supersede all prior versions.

16. Contact Information

Service Desk

Email: Helpdesk@ugt.ge

Telephone: +995 32 2220505

Support Hours: Monday-Friday, 10:00-18:00

Acceptance

By purchasing, subscribing to, or utilizing services provided by UGT, the Customer acknowledges that it has read, understood, and accepted the terms and conditions set forth in this Service Level Agreement.