

შპს სოკარ ენერჯი ჯორჯია

მისამართი: საქართველო, თბილისი, 300 არაგველების ქ.24, 0144

სატენდერო განცხადება

1. ზოგადი ინფორმაცია

შპს სოკარ ენერჯი ჯორჯია (შემდგომში — „შემსყიდველი“) აცხადებს ტენდერს Enterprise Mobility Management (EMM) platform-ის შესყიდვაზე და იწვევს დაინტერესებულ პირებს (შემდგომში — „პრეტენდენტები“) წარმოადგინონ სატენდერო წინადადება წინამდებარე დოკუმენტში მითითებული პირობებისა და მოთხოვნების შესაბამისად.

შესყიდვის საგანია: მონაცემთა კლასიფიკაციის/კატეგორიზაციის სისტემა - Enterprise Mobility Management (EMM) - Workspace ONE Mobile Essentials & Workspace ONE Assist-ის შეძენა, მე-3 პუნქტში განსაზღვრული რაოდენობითა და ტექნიკური მახასიათებლებით.

2. შემსყიდველის რეკვიზიტები

- დასახელება: შპს სოკარ ენერჯი ჯორჯია
- საიდენტიფიკაციო კოდი: 202349440
- იურიდიული/ფაქტობრივი მისამართი: საქართველო, თბილისი, 300 არაგველების ქ.24, 0144
- საკონტაქტო პირი: ლაშა-გიორგი ჭელიძე
- ტელეფონი: +995 591517302
- ელ. ფოსტა: l.chelidze@socar.ge

3. შესყიდვის საგანი და ტექნიკური მოთხოვნები

ქვემოთ მოცემულია შესასყიდი საქონლის ჩამონათვალი მინიმალური ტექნიკური მახასიათებლებით.

Workspace ONE Mobile Essentials & Workspace ONE Assist Functional and Technical Requirements

1. General Requirements

- The **Enterprise Mobility Management (EMM) platform** shall be compatible with the following operating system versions for mobile devices and computers:
 - iOS 11.0+
 - Android 8.0+ (including Android Enterprise)
 - Windows 10, 11
 - Rugged devices
- License Quantity Requirements - The platform shall provide the required licenses (Workspace ONE Mobile Essentials & Workspace ONE Assist) for **1700 mobile devices**;
- The platform shall provide **application containerization** functionality to create an isolated and secure storage environment for corporate data on the device;
- The platform shall support integration with **information storage systems** (network file shares, SharePoint, etc.);
- An **SDK** shall be available for applications developed for Android and iOS, enabling security functionality to be added to the company's existing applications, including:
 - Containerization
 - DLP
 - SSO
 - Network traffic tunneling
 - Login password protection
 - Logging
 - Analytics
- The platform shall support the creation of a **corporate application catalog**. The catalog shall support the inclusion of native mobile applications, web applications, terminal applications;
- **Management console localization** shall be available;
- Officially supported integration with third-party **antivirus, DLP, and VPN solutions** shall be available.
- **First-line software support** should be provided by the software manufacturer for a period of at least **one year**.

2. Requirements for the Enterprise Device Management Platform Components

The system shall include the following components:

- **Mobile Device Management (MDM)** – shall enable rapid enrollment of mobile devices and connection to corporate resources, updating device settings, applying corporate security policies to corporate data and applications, providing secure mobile access to corporate resources, and remotely wiping corporate data from mobile devices.
- **Mobile Application Management (MAM)** – shall enable the creation and management of a corporate mobile application catalog (**App Catalog**) and the management of user access rights to corporate applications.
- **Mobile Content Management (MCM)** – shall provide secure access to work files, documents, and local and cloud-based data repositories. Access to local data repositories shall be provided **without caching data in the cloud components of the solution**.
- **Mobile Email Management (MEM)** – shall provide a high level of security for the corporate mobile email infrastructure.
- **Mobile Compliance Policies module** – shall enable automated responses to risks associated with the theft, loss, or compromise of a mobile device and help prevent **corporate information and data leakage**.

3. Architecture Requirements

- The platform shall support **cloud-based (SaaS) deployment** of device management components;
- The platform shall support **scalability**, allowing the number of connected mobile devices to be increased to **10 000 devices**;

- The platform shall support integration with corporate user directories, including **Microsoft Active Directory, Azure Active Directory/Entra ID, LDAP, Okta**;
- The platform shall support **Single Sign-On (SSO) authentication** on devices;
- The platform shall include a component for **proxying access to corporate email resources from mobile devices**, with the capability to verify the device's compliance status against defined compliance policies;
- The platform shall include a component for **proxying access to corporate content**, including document folders and internal web resources.

4. EMM Management Functionality Requirements

- The platform shall provide functionality for **monitoring and generating automated reports on security policy violations**;
- The platform shall support **user access control for corporate applications and data**, as well as the creation of user groups for efficient application of device settings and access permissions;
- The EMM administrator shall be able to **remotely lock and unlock mobile devices**;
- The platform shall support **remote updates of the EMM client application**;
- The platform shall include a **native managed application** for accessing the corporate **Microsoft Exchange email system and calendar**;
- The platform shall include a **native managed browser application** for accessing internal web resources from mobile devices;
- The platform shall include a **native managed application** for accessing the company's internal file resources from mobile devices;
- The platform shall support the establishment of **encrypted tunnels for access to internal corporate resources on a per-application basis**, individually for each authorized application, without deploying a full-featured VPN client on the device and without using third-party solutions;
- The platform shall provide a **web-based interface** for system administration;
- The platform shall support **role-based access control**, including the following roles: System Administrator, Information Security Administrator, Technical Support Specialist, and User;
- The platform shall support **remote inventory of mobile devices**;
- The platform shall provide access to **statistical information on mobile device user activities**;
- The platform shall support **logging of EMM administrator activities**;
- The platform shall support **multi-tenancy** and the creation of a hierarchical structure of device administration groups;
- The platform shall include its own **Data Loss Prevention (DLP) system**, integrating a secure email client, browser, and file storage into a single ecosystem;
- The platform shall provide a **unified application for corporate use**, displaying the corporate application catalog, notifications, and a customizable home page, as well as providing the ability to search for employees within the organization when integrated with **Active Directory**;
- The ability of **Remote management of mobile devices**, including screen access and file system access, to provide remote user support. This module shall be provided by the manufacturer of the core EMM solution.
- An optional add-on module shall be available for **creating customized reports**. The module is not required in the current configuration; however, it shall be possible to add it in the future **without changing the existing solution**;

5. Data Protection Requirements for Mobile Devices

The functional requirements for protecting corporate data on mobile devices include:

- Mandatory **user authentication** on the mobile device;
- Enforcement of **password length and complexity requirements** for access to the mobile device;
- Functionality for **remotely removing corporate data only (the corporate partition/container)** from a mobile device upon command from the EMM system administrator. This shall enable the removal of confidential information in the event of device loss or employee termination;
- Support for **application containerization** to provide an isolated and secure storage environment for corporate data on the mobile device;
- **Encryption of corporate data** stored on the mobile device's internal and removable storage media;
- The ability to **prohibit and/or log synchronization events** involving data from secure storage with the mobile device or another resource;
- The ability to **centrally apply policies and restrictions** to mobile devices, including configuration of device settings through automatically enforced policies;

- The ability to enforce **security policies in offline mode**, when there is no connection to the management server;
- Protection against applications obtaining **full administrative/control privileges over the operating system**, including detection/prevention of **jailbreaking and rooting**;
- **Encryption of data when accessing corporate resources from mobile devices**, including the establishment of an individual SSL connection between mobile applications and the access gateway;
- The ability to perform a **selective wipe** of data from the mobile device;
- Automatic locking of the mobile device after a **predefined period of user inactivity**;
- Functionality for **wiping all data from the mobile device (factory reset)** when a predefined number of unsuccessful password entry attempts is exceeded;
- The ability to **prevent users from updating the firmware** of mobile devices;
- Functionality for **centralized software installation** on mobile devices, both from public application stores and from applications developed internally by the company;
- Functionality for **blocking software installation from public application stores**;
- The ability to define **software allowlists and blocklists** for mobile devices;
- The ability to **disconnect a mobile device from corporate resources** in the event of a software installation policy violation, with notification to the employee and the employee's manager;
- The ability to access **corporate content**, including documents with version tracking and notifications of new document versions, as well as corporate email with **DLP functionality**, including restrictions on saving and forwarding attachments and copying portions of email messages outside the secure area of the mobile device;
- The ability to define an **application policy specifying access parameters based on networks or specific access points**.
- The ability to define specific **policy for accessing wireless networks**.
- The ability to control corporate devices with **Live location tracking**.

6. Self-Service Portal Requirements

- The ability to **pin a corporate web portal or intranet site to the navigation panel**;
- The ability to **reset the password on a mobile device**;
- The ability to **activate an optional policy on a mobile device from a predefined list**;
- The ability to **access corporate content**;
- The ability to **remotely lock a mobile device**;
- The ability to **remotely wipe a mobile device**;
- The ability to **locate a mobile device**;
- The ability to **trigger an audible alert on a mobile device**.

4. მონაწილეობის საკვალიფიკაციო მოთხოვნები

ტენდერში მონაწილეობის მისაღებად პრეტენდენტმა უნდა წარმოადგინოს შემდეგი დოკუმენტაცია:

1. სამეწარმეო/საგადასახადო რეგისტრაციის დამადასტურებელი დოკუმენტი (ამონაწერი მეწარმეთა და არასამეწარმეო (არაკომერციული) იურიდიული პირების რეესტრიდან).
2. ამონაწერი, რომელიც ადასტურებს, რომ პრეტენდენტი არ იმყოფება ლიკვიდაციის ან გაკოტრების პროცესში.
3. ცნობა საგადასახადო დავალიანების არარსებობის შესახებ.
4. შესაბამისი გამოცდილების დამადასტურებელი დოკუმენტაცია (ბოლო 2 წლის განმავლობაში მინიმუმ 1 ანალოგიური ხელშეკრულების/მიწოდების დამადასტურებელი დოკუმენტი ან/და სარეკომენდაციო წერილი).

5. შეთავაზებული პროდუქციის ტექნიკური სპეციფიკაციები (მწარმოებლის დოკუმენტაცია/სპეც-ფურცელი).
6. შემოთავაზებული პროდუქციის მწარმოებელს (მოწყობილობების შემთხვევაში) საქართველოში უნდა ქონდეს ოფიციალური საგარანტიო მომსახურების სერვის ცენტრი.
7. ავტორიზაციის წერილი მწარმოებლისგან ან ოფიციალური დისტრიბუტორისგან.
8. ხელმოწერილი და ბეჭედდასმული სატენდერო წინადადება, ფასების ცხრილთან ერთად (დანართი №1).
9. პრეტენდენტს უნდა ჰყავდეს შესაბამისი ვენდორის სერტიფიცირებული ქართულ ენოვანი სპეციალისტი.
10. პრეტენდენტი არ უნდა იყოს საჯარო შესყიდვების - procurement.gov.ge შავ საშვი.
11. პრეტენდენტის მიერ შემოთავაზებული პროდუქტი არ უნდა იყოს შექმნილი/ნაწარმოებია ქვეყნის უსაფრთხოებისთვის საფრთხის შემცველი ქვეყნის მიერ.
12. დამკვეთის ინფორმაციული ტექნოლოგიების გარემოში არსებულ მონაცემებზე დაშვების საჭიროების შემთხვევაში პრეტენდენტს უნდა ქონდეს დანერგილი ინფორმაციული უსაფრთხოების მართვის სისტემა და წარმოადგინოს შესაბამისი აუდიტის ანგარიში და კონტროლის მექანიზმების გამოყენებადობის განაცხადი (SOA).
13. პრეტენდენტის მიერ კონტრაქტორის გამოყენების საჭიროების შემთხვევაში აღნიშნული წინასწარ შემოთავაზების წარმოდგენისას უნდა აცნობოს დამკვეთს.

5. სატენდერო წინადადების წარდგენის წესი

სატენდერო წინადადება წარმოდგენილი უნდა იქნეს ელექტრონულად tenders.ge პლატფორმაზე.

დაგვიანებით წარმოდგენილი წინადადებები არ განიხილება.

6. სატენდერო წინადადებების შეფასების კრიტერიუმები

სატენდერო წინადადებები შეფასდება შემდეგი კრიტერიუმების მიხედვით:

შეფასების კრიტერიუმი
სატენდერო წინადადების ფასი
შეთავაზებული ტექნიკის მახასიათებლების შესაბამისობა/გადაჭარბება მინიმალურ მოთხოვნებთან
გარანტიის ვადა და საგარანტიო მომსახურების პირობები
მიწოდების ვადა

შემსყიდველი იტოვებს უფლებას, არ დააკმაყოფილოს არცერთი წარმოდგენილი წინადადება, საჭიროების შემთხვევაში მოითხოვოს დამატებითი ინფორმაცია/განმარტება პრეტენდენტისგან, ან შეწყვიტოს ტენდერის პროცედურა ნებისმიერ ეტაპზე.

7. ხელშეკრულების ძირითადი პირობები

- მიწოდების ვადა: ხელშეკრულების გაფორმებიდან 60 კალენდარულ დღეში.
- გადახდის პირობები: უნაღდო ანგარიშსწორება (საბანკო გადარიცხვა); ჯამური ღირებულების 40% წინასწარ ავანსის სახით, ხოლო დარჩენილი 60%, მიღება-ჩაბარების აქტის საფუძველზე, 10 კალენდარული დღეში.
- გარანტია: მოწოდებულმა პროდუქტმა უნდა უზრუნველყოს პროდუქტების ცხრილში (მუხლი 3) მითითებული მინიმალური საგარანტიო ვადები; მიმწოდებელი ვალდებულია უზრუნველყოს უფასო საგარანტიო მომსახურება/შეცვლა გარანტიის პერიოდში.
- პირგასამტეხლო: მიწოდების ვადის დარღვევის შემთხვევაში მიმწოდებელს დაეკისრება პირგასამტეხლო ყოველ ვადაგადაცილებულ დღეზე ხელშეკრულების ღირებულების 0.01% ოდენობით.
- შესყიდვა განხორციელდება საქართველოს კანონმდებლობის შესაბამისად.

8. დამატებითი პირობები

პრეტენდენტს უფლება აქვს, დასვას დამაზუსტებელი კითხვები წერილობით, ზემოთ მითითებულ საკონტაქტო ელ. ფოსტაზე, მუხლი 5-ში მითითებულ ვადამდე.

წინამდებარე დოკუმენტში ცვლილება/დამატება, საჭიროების შემთხვევაში, ეცნობება ყველა დაინტერესებულ პირს ტენდერის დასრულებამდე გონივრულ ვადაში.

ტენდერში მონაწილეობასთან დაკავშირებული ყველა ხარჯი ეკისრება პრეტენდენტს.

დანართი №1 — სატენდერო წინადადების ფასების ცხრილი

პრეტენდენტის დასახელება: [_____]

საიდენტიფიკაციო კოდი: [_____]

#	დასახელება	ერთეული	რაოდენობა	ერთეულის ფასი (დღგ-ს ჩათვლით)	ჯამური ღირებულება
1	Workspace ONE Mobile Essentials & Workspace ONE Assist	ცალი	1700		
სულ ჯამური ღირებულება (დღგ-ს გარეშე):					

ფასები მითითებულია ლარში (GEL), დღგ-ს ჩათვლით.

პრეტენდენტის ხელმომწერი პირი: _____

თანამდებობა: _____

ხელმოწერა: _____ ბეჭედი: თარიღი: _____