Appendix E – Cyber Requirements

1. General

“System”	The charging management system for bus depots proposed by the Supplier, and further developed in accordance with the requirements of the Agreement;
“Administrator user”	User with full access rights
“Operator user “	User with basic charger controls: start, stop transaction, Charge point Reset
“Viewer user”	User with view only rights

The appendix refers to the requirements for both the production of the System and the Supplier which will install and maintain the System’s processing aspects.

Part 1 - Global and Cloud Security Requirements

2. Commitments

The Supplier is required to meet the following conditions;

2.1 A commitment to meet the requirements of information security, privacy, and cybersecurity (hereinafter referred to as the “Requirements”) that will be set out on behalf of the Company from time to time.

2.2 A commitment to fully comply with the privacy protection requirements of the State of Israel.

2.3 A commitment to secure all information that will come within the framework of this engagement, and to protect the information from any damage or theft.

2.4 The Supplier will deny access to the computer systems in its possession and the computer systems that serve it for this engagement, from anyone who is not certified and authorized to review the material or information stored on these computers.

2.5 Commitment to comply with the ISO27001 or NIST 800-53 data security standard. Completion of the process up to one year from the date of signing the Agreement.

2.6 A commitment to fully impose the Requirements on the sub-providers, including future requirements.

2.7 The Supplier will fully comply with the Requirements of the protection theory for suppliers (supply chain) of the Israel National Cyber Directorate, as a material supplier at level A1 (obtaining certification by an approved institute). https: //www.gov.il/en/departments/news/querysupply.

3. Data Retention

3.1.1 The cloud sites where the infrastructure can be established and the information can be stored and the country to which the personal information is requested to be transferred have privacy laws, which guarantee a level of data protection, which is no less than the level of data protection, which is set out in the Israeli law. List of allowed countries: EU countries, Andorra, Argentina, Canada, Switzerland, Faroe Islands, Isle of Guernsey, Isle of Man. Obligation of the database owner to receive a written commitment from the Supplier that it is taking sufficient measures to ensure the privacy of the information, and that the information will not be transferred to anyone in that country or another country, in accordance with the Israeli Privacy Protection Authority guidelines for transferring personal information about Israelis for computerized processing outside of Israel that are updated from time to time.

3.1.2 The Supplier undertakes to delete the information related to the Company as part of this Agreement at the end of the Period of Engagement, or in accordance with the Company's instructions, without the ability to retrieve, including technical appendices.

3.1.3 The Supplier will ensure that the cloud service provider undertakes that the data managed in the applications that will be stored for the Company remains within the aforementioned countries, and will not be transferred to other countries, including for backup purposes or in the event of a failure of one of the sites.

4. The System shall meet the following standards:

4.1 Compliance with OCPP Security profile 2 requirements.

4.2 The cloud provider is required to be certified to one of the following standards:

4.2.1 AICPA SOC Standard 2/3

4.2.2 ISO/IEC27017

4.2.3 ISO/IEC27018 (Private Information in the cloud)

4.2.4 CSA STAR Level 2

4.2.5 FEDRAMP

4.2.6 SSAE16

or any standard corresponding to the standards set out above and accepted in the country in which the infrastructure will be built.

5. Secure architecture

5.1 Basic assumptions

The protection layers required in the architecture are for all types of cloud solutions (IAAS, PAAS, SAAS, etc.) if the service is in storage/on-premises, additional protection layers will be configured to secure the Supplier's infrastructure.

The protection layers can be part of the service provided in the cloud or as added protection components in the cloud infrastructure.

An alternative solution can be offered that meets all the protection requirements in the proposed layer.

5.2 Architecture security requirements:

Cloud Infrastructure Security

The cloud infrastructure will be secured using several protective layers:

5.2.1 First protection layer – dedicated infrastructure for the System - establishing a dedicated infrastructure for the System or an integrated infrastructure via a separate "instance" and multi-tenant work method with a complete separation in the data management between the clients of the Supplier.

5.2.2 Second layer of protection – protection of the connection – protection against threats of damage to System's survivability / attempted hacking:

a) Implementation of anti-Denial of Service (DoS)/ Distributed Denial of Service (DDoS) application that allows reducing the chance of DoS /DDoS attempts (cloud service)

b) Implementation of an active product that will prevent attack attempts such as Intrusion Prevention (IPS) as part of the firewall.

c) Implementation of an information security policy (hardening policy) to all communication components such as the router, switch, etc.

5.2.3 Third protection layer - separation of infrastructure by firewall (FW) - establishing a dedicated FW for the protection and separation of infrastructure and buffer zones Demilitarize Zones (DMZ-s). The external firewall will have multiple network cards, with the minimum distribution being:

- DMZ Zone I – Internet connection Infrastructure
- DMZ Zone II - Web Server Infrastructure / Control Portal
- DMZ Zone III – Remote connection Infrastructure for providers and administrators (including Authentication Servers)
- DMZ Zone IV – infrastructure for connection to databases / datacenter.
- DMZ Zone V – a connection to the additional firewall that protects the connection to the wider network.
- DMZ Zone VI - connection to the management infrastructure

5.2.4 Fourth layer of protection – application-level access protection:

a) The access will be protected by WAF – Web Application Firewall - that will protect access and applicative hacking attempts.

b) The infrastructure will be built in at least three (3Tier) layers and each layer (display, application, data) will be defined in a separate segment.

c) A gateway component such as Secure Socket Layer / Virtual Private Network (SSL/VPN) to prevent direct access to the System. Priority in accessing the System through an SSL/VPN infrastructure which allows Policy to be downloaded to the user's station.

d) Access to control systems will be performed through MFA (Multi Factor Authentication) authentication – at least two factors (2FA) based on One Time Password (OTP)/SMS, etc.

e) Secure access by HTTPS protocol with SSL TLS 1.2 or higher, with a standard certificate which will be purchased and maintained by the site developer.

f) The System must include a mechanism that will disconnect inactive users after a period of time defined by the administrator

g) The system will allow to proactively disconnect by the Logout button that will return the user to the system screen on the main system.

5.2.5 Fifth Layer of Protection – Operator users / Administrator users and administrators .

a) Implementing an SSL/VPN Gateway component for the Operator users, and Administrator users access. the SSL/VPN will be the primary barrier to access to the infrastructure. The gateway will open an encrypted session between the client and the component.

If possible - on the Supplier's computers, the SSL / VPN component and verify the existing level of security at the endpoints. At the same time, the SSL/VPN component will prevent the user from working on additional systems while working on the infrastructure – that's in order to prevent a hostile party from taking over the station.

b) Intelligent authentication of employees and support and maintenance providers - The gateway will identify the operator users using smart authentication-OTP/token/ card. Users will be defined in a dedicated active directory or alternatively in a dedicated table in the database.

c) The password policy and user management will be performed in accordance with the Company policy, a detailed setting will be in the detailed design phase.

5.2.6 Sixth layer of protection: Protecting the databases of the control system

a) Separate the database from the rest of the integrator clients:

- First (and preferred) option – a dedicated database belonging to the Company will be established for the Charger control and monitoring system.

- Second Option – Separate Application Instance for the Charger Control and monitoring system.
- Third option– implementing a dedicated database as part of a central Instance.

b) The information at rest in both the database and backups will be encrypted using the inherent capabilities of the database or third-party software.

c) The security policy in the database will be implemented in accordance with the database type and Application configuration (including the access to the database).

5.2.7 Seventh Layer of Protection – Protection of the Wide area Network Infrastructure (connection to the chargers):

The protection of the wider network infrastructure will be based on a number of measures:

d) Protection with an internal firewall on the connection to the chargers which will prevent access between the different sites.

e) The connection between the control infrastructure and the charging sites will be performed by encrypting the communication media and authentication between the components.

f) The required encryption level is; for symmetrical encryption AES256, encryption keys for asymmetrical encryption – 2048.

g) The connection will be performed to two sites for failover redundancy purposes (main line and secondary line).

5.2.8 Eighth protection layer – sanitation / filtering system – in order to upload information to the System or to get security and operation updates it is required to integrate a sanitation system that will filter the files that come from the various manufacturers in the infrastructure.

The sanitation system will define the types of files that are allowed to be uploaded to the System, examine all files, disassemble the file, and test its reliability. The Gateway or application must send the file for review, digitally sign it, and upload it to the System.

5.2.9 Nineth Protection Layer - Interface protection layer – All connections to the System will be made in batch format. The initiative in the connection will be from the control system vis-à-vis the external systems. Each connection will require two-way authentication (with a preference for a digital certificate) and communication media encryption. Information security in the connection will be characterized according to the interfaces that will be added.

5.2.10 Tenth Protection Layer: Information Security Events – SIEM infrastructure that will collect all logs from all systems, perform correlation and detect internal and external attack attempts will be established.

5.2.11 Eleventh Protection Layer: Management – The management of the entire systems in the infrastructure (components management - network, systems, etc.) will be performed through a dedicated management infrastructure. There will be no direct access to management infrastructure from the Internet.

5.2.12 Twelfth Protection Layer: Remote Support – If the System requires the manufacturer's access to remote support – access must be performed through: secure access server, VPN infrastructure, MFA smart detection, network media encryption, defining specific access dedicated to the server where the support is required, Applying Handshake protocol – obtaining permission to support, recording the session, Auditing the activities performed as well as servers, with preference for integrating an automatically password management system.

6. Interfaces' security

6.1 Transfer of information to and from the System

If there are interfaces to and from the System, the following guidelines are:

6.1.1 All communication between interfaces will be performed through an encrypted media

6.1.2 Access to the interface will be authenticated or digitally signed.

6.1.3 Messages will be encrypted.

6.1.4 Communication will be Initiated using one-way communication from the System side.

6.1.5 It is mandatory to authenticate the data (logical tests) to ensure that the information is reliable and in accordance with what is required.

6.1.6 The data received from the user will be verified by "trusted kernel" servers and not on the user side.

7. Processes

7.1 Processes

Regarding each of the processes listed in the section below, the Supplier must act as follows: The Supplier must describe the processes in the system in stages from beginning to end. The breakdown must include the system operations, which components the system calls, in which protocols, and security subprocesses – authentication, permissions, etc.

7.1.1 Heartbeat process – all components in the control infrastructure will be monitored by dedicated software. The software will be embedded in the management infrastructure and monitor the livelihoods / utilization of the servers, etc.

7.1.2 System upgrade process – The System upgrade process will be performed in stages, where the software file must be examined through the CDR (sanitation) system and digitally signed by the manufacturer.

7.1.3 The process of updating the charging components – The process of updating the charging components will be performed by downloading the update file to a dedicated server, checking the file and distributing the file to the System after an identified and secure connection and checking that the update passed successfully.

8. Authentication

8.1 Authentication

8.1.1 Operator users

a) Operator users accessing the cloud operations system will use 2FA authentication by using OTP or SMS. The username will be the username defined in Active Directory in the control infrastructure.

b) User policy rules and passwords (Reference to password if password is required to be incorporated as part of authentication and not just the MFA-based authentication):

- Authentication is personal authentication and not group authentication
- A user who failed to authenticate 5 times will be blocked for a set period of time and then will be automatically released
- A user who fails 10 times in half an hour will be locked and will be unlocked manually only after an inquiry.
- The password will be at least 8 characters
- The password will consist letters, number and special characters
- History – Saving history of at least 24 passwords.

c) Failure to authenticate:

- A user who failed to authenticate 5 times will be blocked for a set period of time and will be automatically released
- A user who has failed another 5 times will lock and open manually only after an inquiry.

d) Passwords stored by the system should be encrypted or hashed. Users should not be allowed read permission the password system and certainly not write permission. Password encryption should prevent the system administrator from authenticating themselves as one of the users, even if he can reach the stored passwords. Under no circumstances should passwords be stored within the system code.

e) Sending passwords within the network media (in case of network authentication) should be performed encrypted, either by the Challenge-response mechanism or by establishing an encrypted network media with the system and sending the password within this media.

f) User entry from two stations at the same time is prohibited.

g) Log-out after a period of time without using the system (approximately 20 minutes / X minutes).

8.1.2 Administrators

If the service is a SAAS cloud service, this section is irrelevant.

a) Administrators requires dedicated workstations to access the infrastructure management.

b) All the rules that apply to users apply to the administrators, but the password policy will be more extensive, i.e., the username will be the username defined in Active Directory in the control infrastructure in the remote management/access infrastructure, password policies will be at least 12 characters, etc.

c) Management will be performed by restricting access to the management interface from approved networks / equipment only, encrypting traffic, authentication by two identifiers (2FA), displaying information according to the organization's compartmentalization rules.

8.2 Identifying software components

8.2.1 If applicable, implement a signature mechanism that will not allow an unauthorized software component to run.

9. Compartmentalization and permissions

9.1 General

9.1.1 The System must support compartmentalization and permissions at the infrastructure level.

9.1.2 The authorization application will be against any component of the System that will not be able to run if the user who started it does not have the appropriate permission.

9.1.3 Each user will receive the minimum permission they need to do their job.

9.1.4 Compartmentalization will be performed by implementing RBAC mechanism in all information systems according to the unique authentication of each user and the system's ability to implement the mechanism.

9.1.5 Priority will be given to implementing users on a domain user basis and not on an application user basis.

9.1.6 At least two infrastructure levels of access permissions are required: administrator access and maintenance access. And at least three application level of access permission (as defined in section 7.2 of Volume C).

9.1.7 In accordance with the user's authentication, their affiliation with security groups and the work profile will be determined. Actions that the user is not authorized to perform will not be displayed.

9.1.8 The level of compartmentalization required in the system is based on Need-to know.

9.1.9 It is necessary to save the original files in the database and to prevent the ability to overwrite fields.

9.1.10 A single user besides the database DBA will be defined, this user will be the application (as a service). The database will not be accessed by any other users.

9.1.11 In the database – it is required that the network administrator not have access to the data in the database, but for maintenance purposes only.

9.1.12 The only ones who will be allowed to change system settings are information security managers / infrastructure administrators depending on the level the system sensitivity.

9.1.13 The data received from the user will be verified by "trusted kernel" servers and not on the user side.

10. Encryption

10.1 Encryption of communication media

10.1.1 Information traffic from the charger to the System will be performed in an encrypted manner - encryption of TLS 1.2 or higher.

10.1.2 The connection between the charger and the System will be made using VPN, according to the article in the Architecture section.

10.2 Data at Rest protection

10.2.1 All information that will be stored will be encrypted to a strong level of encryption through inbuilt encryption or alternatively third-party encryption software.

10.2.2 Information encryption is required to be implemented at different layers of the system (e.g., backup encryption, database-level encryption, or storage layer level).

11. Audit

11.1 General requirements

11.1.1 It is required that all actions performed on the system are recorded, including security operations.

11.1.2 Records must be "Tamper proofed", accessible and readable to external systems.

11.1.3 The basic log must include monitoring of all operations performed in the system (applicative logs). Log requirements will be determined during the detailed design for the system connection phase. Basic requirements:

- Monitoring of management actions performed on the system such as system settings, updates, Auditing - starting, stopping, viewing. system's privileges delegation.

- Monitoring all events at both user level and administrator levels, both at the application and operating system levels.

- Monitoring authentication - Success and failure (Login, Logout) of all events, password change/renewal, system permissions - authorization, change of permissions, creating profiles, changing profile setting, and more.

- Input / Output – Monitoring data entry in the system fields, incorrect data entry attempts, entry logging in the database, and more.

- Running services related to the app, Store Procedures, Jobs, Transactions and more. The control - success, failure, time and more.

11.2 Managing the log file:

11.2.1 Log file access permissions – it is required that multiple levels of permission to the log file can be set, log permission levels will be: view, process, copy, delete, and more.

11.2.2 Log maintenance - the log in the system must allow regular maintenance of the log - setting the saved log size, updates, log backup and more.

11.2.3 Transporting the log through an additional security component - there is a possibility that there will be no direct access to the intermediate server from the proposed system and the logs will be required to be sent through additional security measures - no log change will be made when it is transferred through filtering systems, buffering, firewall, encryption and more.

11.2.4 The log will be sent to SIEM system

11.2.5 The monitoring requirements in the system will be in accordance with the monitoring requirements specified in the log writing procedure.

12. Hardening Systems

12.1 Hardening the operating system

12.1.1 Hardening will be performed in accordance with the Company's hardening policy (the hardening policy will be given at the time of detailed design).

12.1.2 Unnecessary services, which are not required for the functioning of the system, will be removed, and will be deactivated as part of a concerted activity to harden the servers and workstations. Full characterization of the necessary services will be performed in cooperation with the organization's information security team in order to avoid functional damage to its system.

In addition, operating systems will be hardened according to the organization's standard hardening procedures, including installing up-to-date antivirus software and automatically updating signature files.

12.1.3 Static, fixed, and specific ports will be used.

12.1.4 Standard protocols approved by information security will be used.

12.1.5 The System will be having to pass an information security check, the satisfactorily pass of the check will be a condition for receiving it in the Company.

13. Software Updates

13.1.1 Any software update is required to be performed in batch form after the update has been downloaded from the cloud.

13.1.2 The update file must be checked before running it - performing a manual and/or automated process that includes testing against spyware and back doors.

13.1.3 Setting the update services IP addresses and creating a secure communication media.

13.1.4 Critical security updates will be implemented immediately after checking that they do not harm the system.

14. Backups

14.1.1 Each component of the System must support a malfunction in another part of the System.

14.1.2 All servers in the infrastructure must be backed up after each security or version update.

14.1.3 Backup of Logs and DB should be done once a day and each backup retained for a month.

14.1.4 Encrypted backups will be saved at different datacenter location than the component location.

14.1.5 It is necessary to keep 6 generations of the information for six months.

14.1.6 One backup version is required to be a cold backup.

15. Secure development and versions

15.1.1 The development of the System should be performed according to the Secure Software Development Life Cycle (SSDLC) methodology. which includes:

a) Protection against known attacks such as: Buffer overflow, cross side scripting, hidden field manipulation, cookie poisoning, SQL injection, backdoors, race condition, dead-lock ,input validation, and more.

b) Development in the configuration of N-Tier.

c) Documentation of the development of the application.

d) Avoiding backdoors.

e) Performing quality control (QC) and quality assurance (QA) tests.

f) Definition of the purpose of the fields and validation (including reference to special characters, etc.).

g) System settings:

1) System settings saved on server only, and in no way on the client computer. In determining how to save settings, pay attention to the protection of sensitive components such as passwords. Additionally, there should be audit on changes to the settings.

2) Version management on the System settings, so that the System can revert to an earlier version in the event of a harmful change in settings – whether if performed in a planned, accidental, or malicious manner.

3) The settings are saved in the Registry file, a text file (or INI), an

XML file, an SQL table, or a combination of all or some of them.

4) logs are written

5) Code and app management including memory management, System permissions, and access control.

6) Implementation of authentication mechanisms

7) Application of authorization mechanisms

8) encryption

9) Digital signature

15.1.2 If the product is not COTS product but a dedicated product developed for the project– the source code must be saved in the vault.

15.1.3 Permissions check will be performed on the server side and not on the client side.

15.1.4 The principle of ”need to know” must be maintained so that the different entities see only what is permitted.

15.1.5 Security procedures for the operating system on which the app is installed must be followed, as well as for any software or hardware involved in the process.

15.1.6 Web pages and all their components (images, connections, login fields, input fields, etc.) must be built according to secure development specifications and be immune from the vulnerabilities published on the top ten OWASP list.

15.1.7 “Delete lock” must be set on all cloud components

15.1.8 At the completion of all the Additional Developments required from the signing date as described in Appendix A2 of the Agreement, , the Supplier must perform a penetration test on all developments in the System. The pen-test must be performed by a third party approved by the Company.

A penetration test will be performed for all developments in the System by a party on behalf of the Company, the supplier must correct all the information security findings that might be discovered in this test, as well as any future test.

16. Sub-suppliers and supply chain threats

16.1.1 It is the responsibility of the Supplier to manage the threats associated with its sub-suppliers, and to perform an ongoing risk analysis on his supply chain. The Supplier will specify which sub-providers are a significant part of the Services and whether the Company's information is transmitted to those sub-suppliers.

17. Ongoing operations

17.1.1 The Supplier is required to conduct a risk management survey of all components used to operate the System and service, starting with physical security of the facilities.

17.1.2 The Supplier is responsible for conducting information security incident detection and response operations for such events, according to their severity.

17.1.3 Supplier is responsible for regular monitoring of the System to identify malfunctions and events.

17.1.4 It is the Supplier's responsibility to perform a periodic scan for weaknesses and vulnerabilities and to install patches as required.

17.1.5 The Supplier is required to perform periodic backups and disaster recovery assessments.

17.1.6 It is the Supplier's responsibility to ensure, inter alia, that accessibility, physically and logically, to the computer facility where the data is stored, will be supervised and audited and that only entities with permission related to the operation and maintenance of the data will be able to access them, provided that those entities have undergone proper training, and has ensured, as much as possible, that there are no offenses related to the prohibited use of the information in their past.

17.1.7 All DBA operations will be monitored at an individual level and unequivocally, and any activity of creation or change in the databases and information will be transferred to the Supplier's information security team.

18. Event Management

18.1.1 It is the Supplier's responsibility to identify information security events and incidents in the System, act quickly and manage the incident fully while maintaining the accepted standards in the field.

18.1.2 The Supplier undertakes that should it identifies a relevant information security event – it will immediately report it to the Company with all the necessary information.

18.1.3 It is Supplier's responsibility to retain all relevant information regarding information security events, including log files, actions performed on the System, response scenarios and System situations in a secure way and without the ability to change it.

19. End of service

19.1.1 Upon the termination of the Agreement, for any reason, the Company retains the ability to export the information in a way that can be recovered in another System and within a reasonable time agreed between him and the cloud provider and the winner of the tender.

19.1.2 In order to avoid lock-in risks, the Supplier will perform the following controls:

a) Document the interfaces and APIs used

b) Periodic export of information from the cloud environment to an external environment, including relevant meta data.

19.1.3 User accounts and access permissions will be blocked after usage is finished.

19.1.4 All information will be deleted at the end of the service. The Company will receive proof from the Supplier about how the deletion was conducted.

ISO27001	Information security standard – International Organization for Standardization
NIST 800-53	Information security standard - National Institute of Standards and Technology
OCPP	Open Charge Point Protocol
IAAS	Infrastructure as a service
PAAS	Platform as a service
SAAS	Software as a service
DoS	Denial of Service
DDoS	Distributed Denial of Service
IPS	Intrusion Prevention System
DMZ	Demilitarized Zone
FW	Firewall
WAF	Web Application Firewall
SSL/VPN	Private Network Safeguard
MFA	Multi Factor Authentication
OPT	One Time Password
HTTPS	Hypertext Transfer Protocol Secure
WAN	Wide Area Network
APN	Access Point Name
AES	Advanced Encryption Standard
SIEM	Security Information Event Management
CDR	Content Disarm and Reconstruction
DB	Database
SSDLC	Secure Software Development Life Cycle
OWASP	Open Web Application Security Project
DBA	Database Administrator