Ayalon Highway- Data security requirements for Suppliers

For Alternative experiment Tender

General

This document presents the information security requirements for the Supplier of the system.

Regulations and Law

The Supplier will appoint a cyber protection and information security officer from the information security team of the Supplier that has the appropriate training in cyber protection and security of information contained in the company's databases stored in the Supplier's systems and services, as required by the Protection of Privacy Law, 1981 and the information security regulations.

The Information Security Officer will be responsible for the implementation of the Cyber Security directives in the field of cyber protection and information security.

The information security officer of the Supplier will maintain ongoing contact with the information security department of the customer.

Compliance with information security standards

The Supplier must comply with the following information security standards:

- Privacy Protection (Information Security) Regulations, 5767 - 2017, regarding the management of databases containing personal information.
- If the Supplier will base the System on cloud services, the supplier must meet the 270001 standard. CSA STAR support Supplier s will be preferred.

Architecture and borders

The Supplier will be responsible for the design of the System to be operated within the project. The design will include all the tools and procedures that will be provided and implemented in the systems, in order to meet the level of information security required in this document. This design will be approved by the company's information security team.

In addition, the Supplier shall establish information security procedures, which will define the areas of responsibility of the Supplier and the Company.

Employee Approval

For all employees who will be accessible to the company and the volunteer's data, a criminal record check and a computer reliability test will be carried out. Only employees approved at the end of this process will be allowed to operate the System.

The Company shall be entitled to demand the replacement of any employee for whom there is a concern of not meeting the conditions and standards to which the Company is obligated.

Development security

The Supplier shall establish procedures that will ensure that the development procedure meets the level of information security required. The procedures shall include, at a minimum:

1. Preparation of a secure code development procedure, which will apply to all the development team. An example of a similar procedure can be found in the Ministry of Health's procedure for the development of secure systems at https://www.health.gov.il/services/tenders/doclib/mi16_2013r.pdf.
2. Appointing an expert for secure development, who will be responsible for assimilating the implementation of the aforesaid procedure in the development processes.
3. Conducting training for all the design, development and testing teams, for all that is required to implement the procedure.
4. Using a computerized tool, such as Checkmarx, to check each code before running it on the system.

Usage of data security components

The Supplier shall make use of the information security components, at the very least:

1. Firewalls, which will be used for partition between networks of different classifications, to protect the interfaces between the client and the central systems operator, to connect to the Internet and external factors, and to split between users and servers.
2. WAF devices for protecting web sites.
3. XML firewall, to protect the interfaces with the customer and with the central systems Supplier.
4. IPS devices, to protect the Internet connection network.
5. DLP devices to prevent the removal of unsecured information from outside the network.
6. Anti-virus software, for all positions and servers on the network.
7. NAC system, to prevent unauthorized access to Supplier networks.
8. SIEM system for collecting, monitoring and analyzing information security events.

Securing Traffic Data

The Supplier is required to transmit information, such as information that passes between the central systems of the Supplier 's systems and between the cellular supplier 's operating systems and at least one of the following: (SSL / IPSEC / VPN / SSH, etc.)

The Supplier will be required to secure the systems by means of protection against DDOS attacks, infrastructure and applications.

The Supplier will provide an advanced security solution that provides advanced monitoring and control capabilities, malicious activity prevention during detection, rest/motion encryption, Capabilities to record and track actions and other changes and other security capabilities that are included in this platform.

Communications

The Supplier will support linkage to the central systems in the following two alternatives:

1. Via the Internet in an encrypted medium. This link will be limited to the company's IP addresses.
2. By means of a designated, encrypted infrastructure between the Supplier and the company, which will enable continuity of work if the Supplier does not have access via the Internet.

Securing Data at rest

Insofar as the Supplier chooses to operate its systems on a public cloud infrastructure, the Supplier will encrypt sensitive information using a standard and recognized encryption algorithm. Sensitive information is information defined as sensitive as defined under the Privacy Law, 1981 or defined by the Company.

For the purpose of implementing the encryption, the HSM system will be used, which will enable the Company to keep the encryption keys which will be under the exclusive control of the Company (desecration and replacement of keys. The Supplier will not have access to the HSM system except for data encryption purposes).

The Supplier must present the company with the data storage architecture to enable the company to identify security risks and controls available to deal with these risks.

Storage and Backup

Information managed on systems will not be exported from the countries which are permitted for personal data storage, according to the instructions of the Ministry of Justice's Privacy Protection Authority. The Supplier's backup site will be subject to the same list.

The systems will be backed up at a frequency of no less than once a day, with backups being stored outside the computer sites.

Access control

Identification:

The Supplier must support at least two of the following means of identification:

• Something you know: A complex password with a minimal length.

• Something you have: Smart Card, RSA Token, One Time Password (OTP) sent by SMS or generated through a phone / other smart device.

• Something you are: Biometric means such as fingerprint, retina, etc.

Passwords:

The Supplier will be required to comply with the following password policy:

- Password complexity: Consists of 8 or more characters including lower- and upper-case letters, numbers, and special symbols.
- Password validity: The password expires after a period of up to 90 days, and the user will then be required to replace it.
- Password history: Keeping a password history of at least 10 passwords backward.

Login and Disconnect

Incorrect authentication attempts using any of these three authentication methods will result in user locking for 15 minutes.

A fixed period of time will be set, after which a communication mechanism will be activated (session time out) that requires the re-identification of the user.

Manage permissions and identities

Access to information must be defined in a precise manner, while granting access permissions only to those whose access to the information is necessary for the performance of their duties.

Mobile Application Security (if such application is provided by the Supplier)

The mobile application will be developed according to the following principles:

1. All personal information, managed on a cellular device, shall be kept in an encrypted form, which will not allow direct access to the data, other than through the application.

2. In order to activate the application, the volunteer must register for the service on the specific device he is using. The application will include measures that will prevent its transfer to another cellular device, without re-registration of the device.

3. Entry into the volunteer's personal data, including travel data and travel history, will require identifying with a PIN code of at least 6 digits or using a fingerprint.

Accessibility to information by the Supplier

The number of entities that can extract all information must be reduced to minimum.

All DBA operations will be monitored individually and unambiguously, and any activity of creating a change in the databases and information will be transferred to the information security team.

Volunteer information shall not be extracted other than way agreed with the company.

Monitoring and Control

The system logs will be collected by a designated SIEM or Syslog system or sent to the company's SIEM system for monitoring and alerting security events occurring on the systems.

The Supplier must enable the company or anyone on its behalf to collect the system records in real time / in a scheduled manner.

The logs will be transferred in the UTC format.

The Supplier undertakes to keep system records back for a period that changes according to the sensitivity of the system and the regulatory requirements that apply to the system.

The supplier must ensure that system records are maintained on a central server managed by a separate staff.

In a case the Supplier changes the system of logs, he must update the company 60 days in advance in for preparations.

The Supplier will be required to monitor services and systems in the following layers:

- Logging monitoring - real-time or retrospective detection of technical or security incidents occurring.
- Performance monitoring - monitoring loads in computing resources.
- General monitoring and monitoring of unusual / hostile activities (failed identification attempts, unauthorized access, double entry attempts, etc.).

Events that will be defined at a high-risk level such as suspicion of foreign access and / or leakage of information from the database, the Supplier will immediately update the company (according to a specific checklist) and inform the manner of handling them.

Review

At least once every 18 months, the Supplier shall:

• Penetration tests. These tests will be performed by a dedicated specialized company, which was not involved in the process of setting up the systems.

• Comprehensive risk survey.

The results of the surveys and assessments will be presented to the Company at an annual meeting. The Supplier must present a plan for correcting the findings as necessary. In the event of material defects that directly affect the Company's systems, the Company shall be immediately informed of the existence of the defect.

The Supplier will enable representatives on behalf of the Company to conduct a tour of its relevant facilities for information security audits and compliance with agreements and / or contracts signed with the Company.

Lockdown Prevention

The Supplier will enable the Company to maintain a local copy of all information in the Company's facilities and / or any other site of the Company.

Termination of contract with Supplier

Upon termination of the contract with the supplier, the Supplier is responsible for performing the following actions:

- One-value erasure, unrestorable for all data and information stored in the systems.
- Destruction of copies of the data and information used as part of the Supplier 's activity for the Company.
- The Supplier will be required to show evidence that the information has been destroyed (relevant records and reports).
- If the information is encrypted - Revoke the encryption keys and delete them.