Atarjamat
Privacy policy & Procedures

This website is owned and managed by Atarjamat. We take our responsibilities regarding the protection of personal information very seriously.

Purpose of this policy

We respect your privacy and take the protection of Personal Information very seriously. The purpose of this policy is to describe the way we collect, store, use and protect information.

This policy explains:

Why we need your personal information

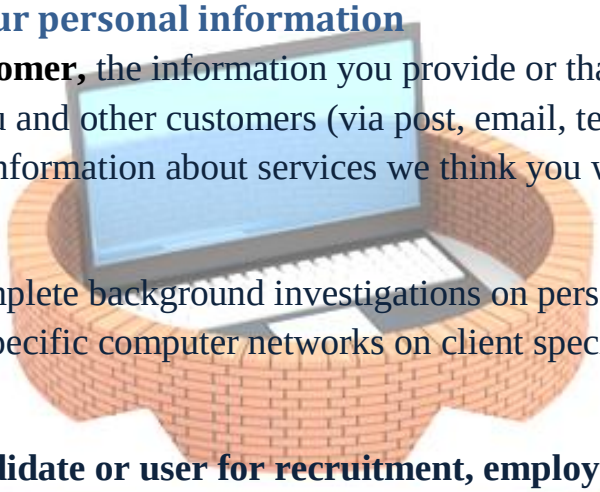
When you will use our services provided, you will be asked to provide certain information such as your name, contact details.

We will store this information and hold it on computers, computerized storage centers or otherwise. We will use this information, by way of example, in some and/or all of the following ways:

- to fulfill our agreement with you, or contacting you if there is a problem
- to answer any queries which you may send to us by e-mail;
- in order to conduct customer satisfaction surveys;
- to meet our legal compliance obligations;
- for recruitment and careers purposes
- for human resources management and employment matters.

How we use your personal information

If you are a customer, the information you provide or that is obtained by us, to provide you and other customers (via post, email, telephone or otherwise) with information about services we think you will find valuable.



We Conduct Complete background investigations on personnel having access to client specific computer networks on client specific information systems.

If you are a candidate or user for recruitment, employment and/or human resources purposes, the information and/or data that you provide

or that is obtained by us on this website or otherwise, will be used by us and/or our affiliates to process your query, request or application. We may also inform you about any relevant opportunities or services, where you have registered to receive these.

We may contact you by post, email, telephone (including SMS) or fax for these purposes. We may also use and analyse the information and/or data that we collect so that we can review, administer, support, improve and develop our business and the services which we offer.

To whom we disclose your personal information

Atarjamat does not sell or trade your personal information to third parties.
If you are a customer,

Sharing: We do not share your Personal Information nor any data related to your business.-

Law enforcement: We may disclose your data if required-

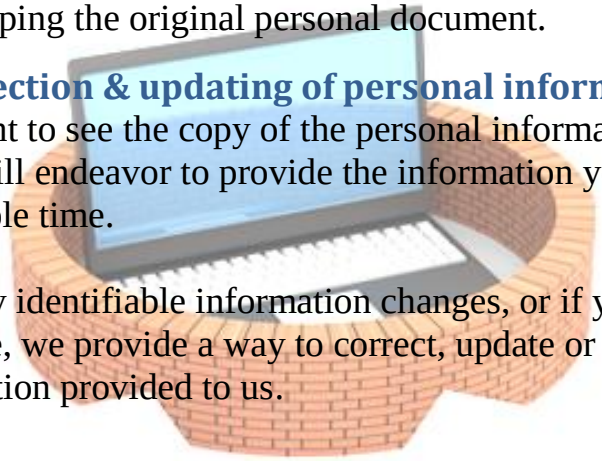
- by a subpoena or court order;
- to comply with any law.

- Employees: We may need to disclose specific data to our employees that require accessing your data to do their jobs.

If you are a candidate or user for recruitment, employment or human resources purposes, only copy of your personal data (including sensitive personal data) has been provided to us for the purposes of enquiring about a position or opportunity, making an application for a position, registering your interest in a career with Atarjamat and other direct or indirect purposes associated with or incidental to the recruitment/careers and/or human resources process with Atarjamat. We never require keeping the original personal document.

Access to/correction & updating of personal information

You have the right to see the copy of the personal information we keep about you. We will endeavor to provide the information you require within a reasonable time.



If your personally identifiable information changes, or if you no longer desire our service, we provide a way to correct, update or remove your personal information provided to us.

Security of Personal Information

We use computer safeguards such as firewalls to protect Personal Information. We also follow strict security procedures in the storage and disclosure of information which you have given us to prevent unauthorised access. Should we be required to disclose sensitive information to you, we may request proof of identity in adherence with our security procedures before we are able to do so.

Data Protection Manager

The data Protection manager develops, implements and maintains risk management and compliance systems in the Legal and Compliance department. He carries out advisory and supervisory the HR, the employees having access to the clients' data, with a high amount of monitoring, reporting, planning and coordination. He also engages proactively in continuous improvement and review of all compliance systems and policies.

Reporting and Investigations:

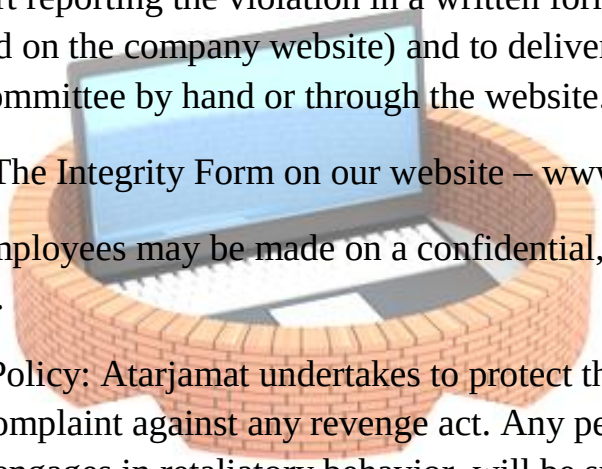
Obligation to Report:

In order to protect employees and avoid legal exposure, employees should report any concerns about violations of the Code and take appropriate remedial actions when violations are discovered.

Filling a Complain:

If the employee notices any violation of this code or any regulations, he/she should start reporting the violation in a written form (using the form uploaded on the company website) and to deliver it directly to the integrity committee by hand or through the website.

-You Can Find The Integrity Form on our website – www.atarjamat.com



Complaints by employees may be made on a confidential, anonymous basis.

Non Retaliation Policy: Atarjamat undertakes to protect the employee who is filling a complaint against any revenge act. Any person, regardless of position, who engages in retaliatory behavior, will be subject to disciplinary action.

Incident Management Reporting

All employees must promptly report potential incidents to the appropriate individual with delegated authority. At the direction of the individual with delegated authority, or his or her designee, workforce members must provide full assistance as needed with the incident management processes.

Incident Management Oversight

On behalf of the institution, the following individuals are responsible for the oversight, direction, and decisions related to investigations and notifications:

1- President

2- Data protection manager

Incident Management Process

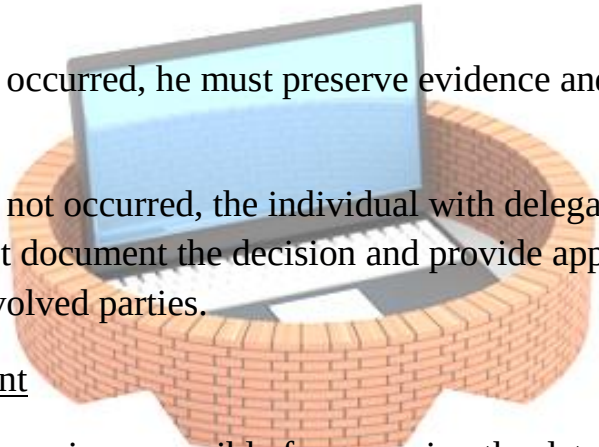
Each individual with delegated authority for incidents or, having access to data is responsible for developing, maintaining, and following an incident management process through the following elements:

A.Assign Incident

The delegated person is responsible for managing the incident.

B.Identification and Preservation of Evidence

The delegated person must investigate to be sure the incident has really occurred.



If an incident has occurred, he must preserve evidence and document processes.

If an incident has not occurred, the individual with delegated authority for the incidents must document the decision and provide appropriate notification to involved parties.

C.Risk Assessment

The delegated person is responsible for assessing the data involved, the risk to the company, and the potential harm to the clients. He is

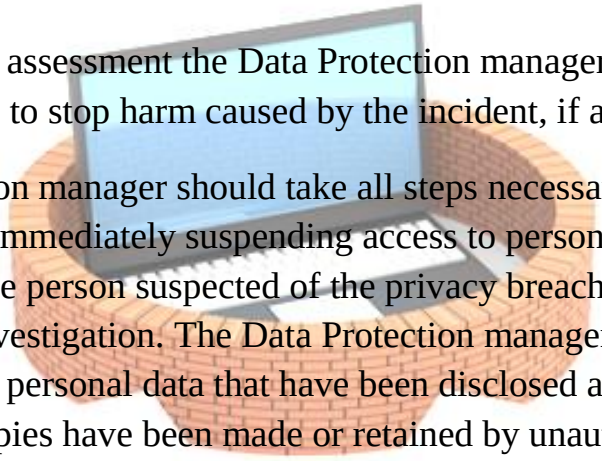
responsible for engaging other areas of the company during the assessment process, as needed, to determine:

• Potential legal, regulatory and financial risks.

• The party (client, employee or supplier) that may be required for next steps based on the circumstances involved in the incident.

- Preventing or Reducing the Risk of Unauthorized Access
- Restricting access to personal data on a need-to-know basis.
- Identifying the person responsible who can access any private information (HR employee for staff records, staff member who must have access to the client's data).
- Revising or revoking access to personal data when the required level of access changes.
- Maintaining a log of staff members who have access to personal data and the Data Protection manager will be responsible for maintaining the log.
- Setting out additional physical, technical and administrative measures to limit the access to personal data: strong password controls to help minimizing the risk of unauthorized access.
- Staff members should also be prohibited from writing down or sharing their passwords and unique user IDs and should be required to change their passwords on a regular basis.
- Staff members should also be required to log off from their computers after working hours.

D.Containment



Based on the risk assessment the Data Protection manager is responsible for taking actions to stop harm caused by the incident, if any.

The data protection manager should take all steps necessary to contain the privacy breach: immediately suspending access to personal health information by the person suspected of the privacy breach, pending the outcome of an investigation. The Data Protection manager should retrieve all hard copies of personal data that have been disclosed and should ensure that no copies have been made or retained by unauthorized persons. The Data Protection manager should determine whether the privacy breach would allow the unauthorized collection, use or disclosure

of any other personal data and take steps to ensure that additional privacy breaches cannot occur through the same or similar means.

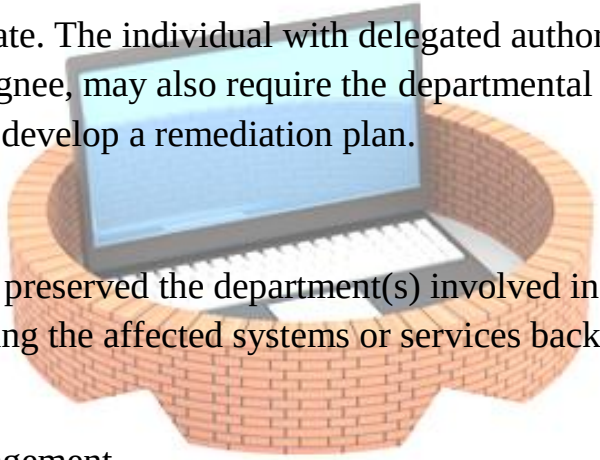
E.Communication and Notification

Communication and notification to persons or third parties affected by an incident will be made as directed by the Data Protection manager and are to be carried out in accordance with applicable legal, regulatory, or contractual requirements.

When notifying individuals about a privacy breach, the Data Protection manager should provide individuals with the following information: • The name of each agent who caused the privacy breach; • The date and time of the privacy breach; • A description of the nature and scope of the privacy breach; • A description of the personal data that was subject to the privacy breach; The measures implemented to contain the privacy breach; • Notice that, following the investigation, the Data Protection manager will provide the individual with a summary of the results of the investigation and the measures that have been or will be implemented to remediate the privacy breach and to prevent similar privacy breaches in the future; • The steps the individual can take to protect his or her privacy or to minimize the impact of the privacy breach; and • The name and contact information for the person to whom the individual may address inquiries and concerns (including police (cyber crime dep, starting case trial …etc.)

F.Mitigation

Efforts to address the weakness that caused the incident may begin at any time, as appropriate. The individual with delegated authority for incidents, or designee, may also require the departmental unit(s) involved in the incident to develop a remediation plan.



G.Recovery

Once evidence is preserved the department(s) involved in the incident may begin restoring the affected systems or services back to an operational state.

H.Records Management

For all incidents, the delegated person must prepare a written summary that includes the pertinent details of the incident and serves as the final and official record for the company to be maintained.

Personal Data update

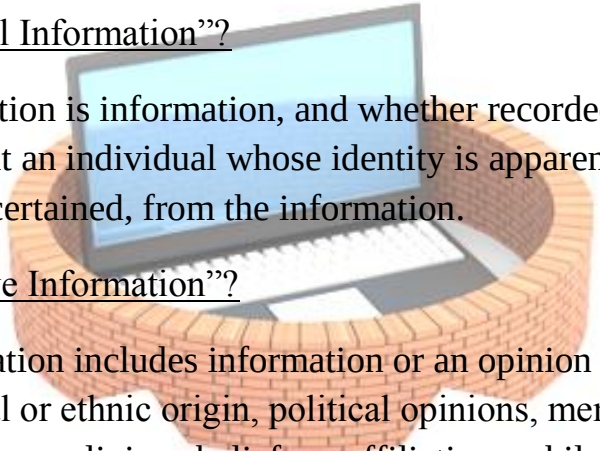
Any client/employee may have access to their personal information (phone, address, email…) to correct, update, change or delete certain data.

Atarjamat should be notified of changes in marital status, number of dependents and beneficiaries, in order to assure proper benefits administration.

Changes to the privacy policy

If we decide to change our privacy policy, we will post the changes on our website so you are aware of what information we collect, how we use it and under what circumstances, if any, we disclose it. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify you by way of an e-mail. You will have a choice as to whether or not we use your information in this manner.

Procedures



What is “Personal Information”?

Personal Information is information, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information.

What is “Sensitive Information”?

Sensitive Information includes information or an opinion about an individual’s racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade

union, criminal record, biometric information, biometric templates, health information about individual and genetic information.

What is “Health Information”?

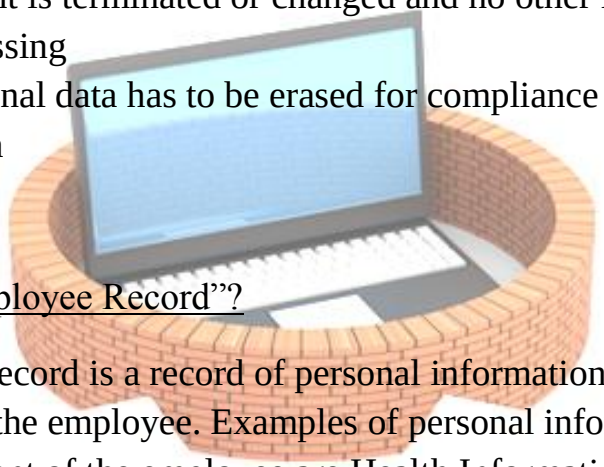
Health Information is: I. information or an opinion about: a) the health or a disability (at any time) of an individual; b) an individual’s expressed wishes about the future provision of health services to him or her; a health service provided, or to be provided, to an individual that is also personal information; or II. other personal information collected to provide, or in providing, a health service; III. other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or IV. genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

What is “Unsolicited Information”?

Unsolicited Information is all personal information received from an individual that we did not actively seek to collect.

The client/employee shall have the right to obtain the erasure of personal data concerning him or her without undue delay and Atarjamat shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- Agreement is terminated or changed and no other legal ground for the processing
- The personal data has to be erased for compliance with a legal obligation



What is an “Employee Record”?

An Employee Record is a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are Health Information about the employee and personal information about all or any of the following:

I. the engagement, training, disciplining or resignation of the employee;
II. the termination of the employment of the employee;

III. the terms and conditions of employment of the employee;

IV. the employee's personal and emergency contact details;

V. the employee's performance or conduct;

VI. the employee's hours of employment;

VII. the employee's salary or wages;

VIII. the employee's membership of a professional or trade association;
IX. the employee's trade union membership;

X. the employee's recreation, long service, sick, personal, maternity, paternity or other leave;

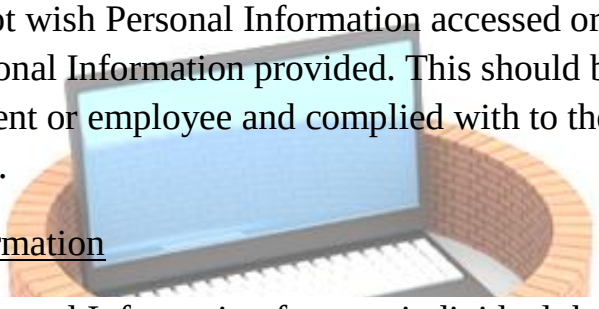
and XI. the employee's taxation, banking or superannuation affairs.

Methods of Collection

We will collect Personal Information from the client or employee in case:
I. we have the consent of the client or resident employee to collect the information;

or II. we are required or authorised by law to collect this information;

or III. At admission, a client or employee should identify any parties from whom they do not wish Personal Information accessed or to whom they do not wish Personal Information provided. This should be recorded in the file of the client or employee and complied with to the extent permitted by law.



Unsolicited Information

If we receive Personal Information from an individual that we have not solicited or if we receive a right to be forgotten request, we will destroy or de-identify the information as soon as practicable and in accordance with the law.

Staff records

We must keep a record in respect of staff about:

I. basic employment details such as the name of the employer and the employee and the nature of their employment;

II. pay;

III. overtime hours;

IV. termination of employment (where applicable);

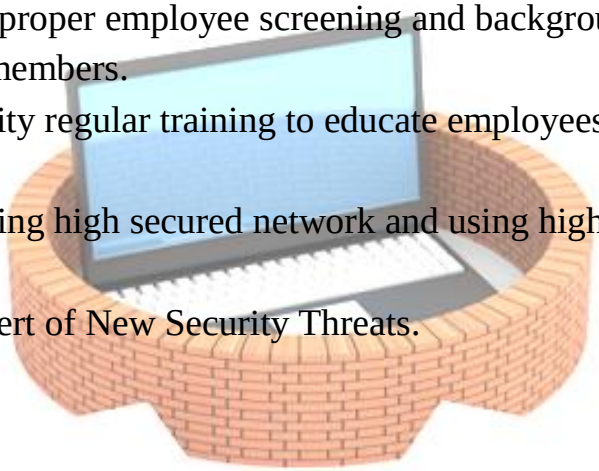
and V. annual leaves.

We may also collect Personal Information about a staff member relating to their employment being Employee Records (as defined above).

Personal Information from an individual that we have not solicited, we will, if it is lawful and reasonable to do so, destroy or de-identify the information as soon as practicable.

Privacy obligations for customer data

- Use a secure file-sharing and messaging platform: using the client mail platform**.**
- Store physical documents (if any) in an environment with high controlled access**.**
- Following proper employee screening and background checks on new staff members.
- Staff security regular training to educate employees on cyber attacks.
- Implementing high secured network and using high advanced server.
- Staying Alert of New Security Threats.



Personal Data update

In order to change the personal data (home address, telephone number, email address…) the client/employee should show current ID, valid passport or driving license prior their access.

Changes to name, marital status, military service, etc. must be made in writing and sent to the HR.

In order to complete the changes procedures, a valid governmental document, showing the new data should be presented.

Regulations on suppliers' potential access to private data

Suppliers acknowledge and agree that the agreement with Atarjamat is made under the Egyptian applicable Data Protection Laws.

The Supplier agrees, warrants and covenants:

(a) to process Personal Data only:

(1) at all times in compliance with Egyptian Data Protection Laws, and solely on behalf of Atarjamat and in accordance with its documented instructions, unless otherwise required by Egyptian Data Protection Laws; and

(2) for the sole purpose of executing the Agreement or as otherwise instructed by Atarjamat, and not for the Supplier's own purposes or other commercial exploitation. For clarity, Supplier will not collect, retain, use, or disclose Personal Data for any purpose other than as necessary for the specific purpose of processing Personal Data, including collecting, retaining, using, or disclosing Personal Data for a commercial purpose other than providing and enhancing Products and Services. Without limiting the foregoing, Supplier will not, except as permitted by the Egyptian Data Protection Laws: (i) use Personal Data for the purpose of Personal Data; (iii) collect, use, disclose, or otherwise process Personal Data for Targeted Advertising; (iv) combine or commingle Company’s Personal Data with Personal Data that Supplier receives from or on behalf of another company(ies), person(s), or Data Subject(s), or that Supplier collects from its own interaction(s) with other company(ies), person(s), or Data Subject(s).

(b) if it is legally required to process personal data otherwise than as instructed by Atarjamat, to notify Atarjamat and the data subject before such processing occurs, unless the Egyptian Data Protection Law requiring such processing prohibits the Supplier from notifying Atarjamat on an important ground of public interest, in which case it shall notify Atarjamat as soon as that Egyptian Data Protection Law permits it to do so.

(c) Further, if supplier determines it has not met or can no longer meet its obligations under Egyptian Data Protection Laws, Supplier will immediately provide written notice thereof to Atarjamat, and (ii) Atarjamat has the right to take any steps it deems reasonable and appropriate to stop and remediate any unauthorized use or processing of personal data, including (without limitation) by terminating the Agreement or any Service provided.

(d) In addition to (and without limiting) any confidentiality obligations, the supplier will treat all Personal Data as confidential information, subject to at least the level of confidentiality and protection supplier applies to its own confidential information, and will not disclose such confidential information without Our prior written consent except: (1) to those of its personnel who need to know and/or have access to the confidential information to carry out the Services; and (2) where it is required by a court, governmental or public authority, or legal process to disclose and/or grant access to Personal Data.

(e) Upon termination or expiration of the agreements, supplier shall destroy all data in its possession or control within 15 calendar days. This provision shall not apply to the extent that supplier is required by any applicable law to retain some or all of the Data, in which event supplier shall isolate and protect the Data from any further processing except to the extent required by such law.

(f) Supplier shall implement and maintain reasonable and appropriate physical, technical and organizational measures to ensure the ongoing integrity, confidentiality and availability of data, and the resilience of systems and services Processing Data, as appropriate to the nature and scope of his activities and services, and in accordance with Applicable Data Protection Law. Such measures will include, without limitation,

protecting the Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, or unauthorized disclosure or access (a "Security Incident"). Supplier will implement and maintain comprehensive and written privacy and information security policies and procedures and provide such documents in ten business days upon written request to Atarjamat. Atarjamat shall have the right to have the service audited.

International data transfer

Any data transfer will comply with Data Protection Laws.

Restricted Transfers from Egypt: If Restricted Transfers of Personal Data subject to the Egyptian Data Protection Law, are made by or on behalf of Atarjamat to client, the Parties agree that all such Transfers shall be governed by the Egyptian Data Protection Law, which are hereby executed and entered into by and between Atarjamat and clients.

Personal data transfer must comply with the relevant mechanism which authorises the lawful international transfer of data according to the Egyptian Data Protection (https://www.trade.gov/market-intelligence/egypt-data-protection).

Right to be forgotten

The data subject shall have the right to obtain the erasure of personal data concerning him or her without undue delay Atarjamat shall have the obligation to erase personal data without undue delay" if one of a number of conditions applies. "Undue delay" is considered to be about a month. Atarjamat must also take reasonable steps to verify the person requesting erasure is actually the data subject.

This process should be completed through the following steps:

- Step 1: submit a right to be forgotten request.
- Step 2: Prepare your right to be forgotten Notice.
- Step 3: Consider your Notice as an appeal to a right to be forgotten refusal.

Security measures

Our security measures include, but are not limited to:

I. **periodical awareness trainings given to our new/old staff** on their obligations with respect to the Personal Information concerning clients or employees;

II. **use of passwords** when accessing the databases system;

III. **use of firewalls and virus scanning tools** to protect against unauthorised interference and access;

IV. **Very limited access** to the personal records.

V. If Atarjamat will need to work, in the future, with a third party entity that might have access to its own data, Atarjamat, in this case, **will make prevent any access to its clients' data**, security and privacy.