Protection of Personal Information Act Policy

PROTECTION OF PERSONAL INFORMATION ACT (POPIA) POLICY

1.1. Policy brief & purpose

The ATS Protection of Personal Information Act (POPIA) policy outlines the organisation‘s guidelines and provisions for complying with the POPIA enforced by the South African government.

1.2. The POPIA role players

The role players are the individuals who are impacted by the POPIA as well as the individuals who are responsible for ensuring compliance. The following are the ATS POPIA role players:

- Data subjects: The data subjects are the individuals whose information ATS records and stores in a structured, unstructured or hard copy format. These include, candidates, Alumni, clients, vendors/suppliers and employees.
- Information officer: According to the POPI Act by default it is the organisation‘s CEO, who is responsible in ensuring that all personal information is processed accordingly and complies with the POPI Act. The information officer is also responsible for notifying regulator when there is a security breach. Currently the information officer is Onyi Nwaneri.
- Regulator: The regulator is the person appointed by the South African government to whom we report when data subjects’ personal information has been compromised at ATS. Data subjects can also report any breaches of their personal information by ATS to the Regulator.
- Data processor: These include the, project managers, project administrators, project coordinators, HR, finance and IT personnel. This is the party that will be receiving and processing data subjects’ data.

1.2.1. Departmental role players

The following is a list of the type of personal information that ATS departments collect and store:

- IT: This departments runs reports that contain data subjects’ personal information includes names, ID numbers, email addresses and contact numbers.
- Sales and Marketing: The sales department processes with clients’ personal information includes names, ID numbers, banking details, email addresses and contact numbers.
- Finance: This departments processes employees, suppliers/vendors, clients and candidates’ personal information which includes names, ID numbers, banking details, email addresses and contact numbers.
- Project Managers: Manage the various programmes offered by ATS which include Bursaries,

Learnership, internships, specialised/ demand driven skills training and Work Experience. As such their business units' process candidates and clients information namely ID numbers, names, banking details, email addresses and contact numbers.

1.3. Scope

This policy applies to all ATS stakeholders who include ATS employees, clients, suppliers, candidates, alumni.

1.4. Conditions for lawful processing of personal information

1.4.1. Accountability

This pertains to ensuring that POPIA conditions set out are complied with and there is a person responsible for that.

- The responsible party (CEO) is the data protection officer and must make sure that conditions set out are complied with.

1.4.2. Processing limitation

This refers to the conditions and purpose of information collection and processing. The following processing limitations will apply:

- Project administrators processing candidates' information must do so in a manner that does not infringe the privacy of the candidates. In order to achieve this the following will be ensured:
    1. The data processor must have a valid reason for processing the information
    2. The data processor must ensure requests by candidates not to have their information processed by ATS is actioned.
    3. The data processor must not process information for candidates who are blacklisted.
- ATS should have in place the following:
    - ✓ consent from the data subjects,
    - ✓ a privacy protection policy on the ATS website and
    - ✓ consent for candidates to agree to the use of their data
    - ✓ Structures to ensure that all candidates who submit their CVs and apply for positions via web portals consents that ATS processes their personal information.
- When the data subjects are no longer with ATS, information will not be deleted from the ATS database but rather, it will be archived on systems for historical reporting purposes. However, ATS data processors will not process the information e.g. sending email or SMS notifications, unless they get renewed consent to do so.

- Consent and privacy agreement document should be signed off when data subjects sign a contract with ATS.

1.4.3. Purpose Specification

This defines how personal information and also information that is no longer in use will be stored or destroyed. And this includes but not limited to the following:

- Clients, candidates and suppliers may withdraw consent to use of information at any time. Upon receiving a request from the data subjects to have their information withdrawn, the ATS responsible party must be notified and the request must be actioned appropriately.
- If clients, candidates, suppliers and employees have objected to the processing of personal information, the protection officer may no longer process the information.
- All ATS data processors must archive information in a secure manner and ensure security of the application systems.
- Hard copy documents should be archived securely in a safe or locked up cabinet that has access restrictions.
- Hard copy information that is no longer required should be shredded, all centers will have shredders in place.
- The destruction of personal information that is on old laptop hard drives or old server hard drives should be done securely in order to prevent its reconstruction in an intelligible form.

1.4.4. Information Quality

This refers to the accuracy in which collected and processed information should be in. All data subjects' personal information must be collected and captured correctly. The following information quality aspects will apply at ATS:

- Data processors responsible for processing and storing data must ensure that personal information is complete, accurate, not misleading and updated when necessary.
- Data processors will capture and regularly conduct quality check on candidates or clients' personal information.
- If the data processor is not sure about the information, they will contact the data subject to verify information and update it accordingly.

1.4.5. Openness

ATS undertakes to be open to the data subjects about which of their information that ATS has and what it is used for. The following will apply in order to be able to maintain openness:

- The data processors will maintain all documentation of any processing under its responsibility. The privacy policy signed will inform data subjects on the information that is being stored.
- The policy will also include what information is being stored and for what purpose
- The data subject can request details of their personal information that is stored by ATS. When a data subject requests a report of their information, ATS data processor will be contacted and records the request, does a verification check of the data subject and responds with the relevant information. The information officer will also be notified of any information requests.

1.4.6. Security safeguards

This section covers the technical and non-technical security measures applied by ATS to prevent any breach of the data subject 's personal information. Below is a list of applied measures:

- Structured data includes the information in various ATS system databases. Application systems should have strong passwords to access them.
- ATS will have a password policy where staff must change their domain passwords every 90 days.
- Unstructured data includes files that are stored on computers and servers. ATS computers will be encrypted using Windows Bit locker.
- Unstructured data should be saved on the ATS server's shared folders for security.
- All ATS Computers should have an anti-virus software. Currently the windows defender is being used.
- Cyber security training will be sent out weekly to ensure that all data processors are aware of cyber security, constantly practice and develop good cyber security habits in order to protect data subjects' information
- Penetration tests should be conducted to determine if there are any security breaches within the organisation.
- Only authorised personnel will have access to the server room and relevant folders on the Server
- ATS has a cyber security policy in place that ensures protection of data subjects' personal information from cyber security threats

1.4.7. Notification of regulator when there is a data security breach

This addresses the measures that are taken by ATS in case of a breach of data subject's information. If there is a security breach of information at ATS, the following will apply:

- The data protection officer (CEO) is notified by the personnel who identifies the security breach.
- The data protection officer will in turn notify the regulator.
- There will be an Incident response policy in place that will followed in case of a security breach in order to mitigate the risks and resolve the issue.

1.4.8. Processing of Children's personal information

In the POPIA, children are any data subjects who are below the age of 18. For any children's information being processed at ATS, the following will apply:

- Afrika Tikkun Bursary Management candidates who are 17 years old will need to have a consent form signed by their parents and guardians for their information to be processed.

1.4.9. Designation and delegation of deputy information officer

The Information Officer will appoint a deputy information officer. Currently the deputy information officer is the IT Manager.

1.4.10. Rights of data subjects regarding direct marketing

ATS will abide by the following in order to directly market to data subject in a compliant manner:

- All candidates who upload their CVs or apply for positions online will be required to accept a privacy policy on the web portals that they use which gives ATS their consent to send email and SMS notifications**.**
- All ATS data processors will need to update any candidate's information and remove those candidates who request to opt out of any mailing or SMS notification lists. This will ensure that notifications are sent via email or SMS to only those candidates who consent to receiving notifications.
- ATS data processors will make sure that all candidates information in the various information systems or unstructured files is accurate so that when bulk SMS or emails are sent they are sent to the correct people.
- All clients and suppliers need to be asked to sign a consent form for them to receive any marketing information via email or SMS so that when these are sent to them ATS will be compliant. **1.4.11. Tran's boarder information flows- do we have any clients outside SA who request candidates inform?**

All ATS clients should agree to keep candidates' information confidential when they receive reports pertaining to the candidates. All clients who receive reports that contain candidate's information will be given a privacy policy to sign that ensures that they agree to the organisation's privacy policy in protecting the candidates' personal information.

I have read the contents above and they have been explained to me. I accept the guidelines above.

Signature: _____

Date: _____