ADMINISTRATION

POLICY: 109

SUBJECT: SECURITY AND DISCLOSURE

PURPOSE: This policy has been developed to meet the requirements of the State of California, Department of Justice, Bureau of Criminal Identification and Information, Field Operations and Record Security Section and any other entity that requires security of confidential information. Sensitive data will be handled, stored, transmitted or destroyed securely to preclude loss or misuse.

POLICY:

1. An employee of SHELTER, Inc. may access employee/client or Agency information only when necessary to perform work specific to their job functions. An employee may NOT access or use information from client, employee, or Agency files or databases for personal reasons or any other reason that falls outside of assigned tasks performed by an authorized employee.

2. Employees may disclose confidential information from client, employee, Agency files, or data bases only to individuals who have been authorized to receive it through appropriate SHELTER, Inc. channels with signed authorization. An employee shall not divulge or make use of confidential information, data or records of the Agency for any purpose unless the same have been authorized. Any misuse is against California law and will be prosecuted accordingly.

3. An employee may not deliberately enter false or incomplete data or delete existing valid data on any of the databases or files. Nor, may an employee deliberately take an unauthorized action that would adversely affect the performance of the data system, or cause the interruption of electronic data processing services, or the destruction or alteration of data files or software.

4. Criminal Offender record information shall be accessible only to the human resource staff and/or hiring authority charged with determining the suitability for employment of the applicant. The information received shall be used by SHELTER, Inc. solely for the purpose for which it was requested and shall not be reproduced for secondary dissemination to any other employing or licensing agency.

5. As a precaution against misuse or destruction of criminal record information, an employee will not remove any work related materials from the work site without specific authorization to do so. Work in process is to be stored (secured in locked drawer/files) and maintained in areas designated as appropriate for such storage and maintenance.

6. Upon determination of an applicant's fitness, the records shall be destroyed to the extent that the identity of the individual can no longer be reasonably ascertained

7. When criminal offender record information is destroyed, the destruction shall be carried out to the extent that the identity of the subject can no longer reasonably be ascertained.

8. An employee must take reasonable precautions to protect computer systems and equipment from unauthorized access. Reasonable precautions include the following: ensure that each computer is inaccessible when leaving it unattended; store user documentation to sensitive programs/information in a secure (secured in locked drawer/files) place; and report any suspicious circumstances or unauthorized individuals observed in the work area to a manager.

FORMS USED: Criminal Justice Information form
DMV Record form

APPROVAL SIGNATURE: _____

DATE: June 2018