The Background Screening Credentialing Council

OPINION LETTER

The Background Screening Credentialing Council has drafted the following response to a question we have received regarding the US Employment Screening / General Background Screening BSOAP Standard, this letter applies to US Version 2.0, 3.0 and General Version 1.0. This response is provided for *educational purposes only* and does not constitute legal advice, express or implied, of the BSCC, or the Professional Background Screening Association. Consultation with legal counsel is recommended in all matters of employment law.

For the purposes of this Letter, and to ensure our response applies to both Standards, the terms Organization and CRA may both be used.

TITLE: Clause 1.6 – Access Protocol

Question: My question is regarding the "attributes of and suggestions for onsite audit" comments for clause 1.6:

Records of access protocol issuance must be securely maintained.

We use a program that creates an encrypted "vault" in which we store all employee passwords. Is this sort of practice what this comment is referring to? If not, would you be able to clarify what would constitute a securely maintained record of issuance?

Response: Thank you for your inquiry.

Specifically, you state "We use a program that creates an encrypted "vault" in which we store all employee passwords.

An encrypted vault for the storage of Employee passwords may be one component of user access protocols and controls, but that alone is not sufficient to satisfy Clause 1.6. A fuller response to your inquiry is provided below.

Clause 1.6 reads as follows:

1.6 Access Protocol

Organization/ CRA must have and follow procedures requiring use of secure access protocols for Organization/CRA workers, authorized client users and any other authorized users accessing Consumer Information. At a minimum, procedures must meet all applicable legal and regulatory requirements.

The standard with Audit Criteria goes on to state:

Organization/CRA must demonstrate that access to consumer information by Organization/CRAworkers and authorized clients users is controlled. Acceptable access protocols may include, but are not limited to, strong passwords, biometric identification, and/or multi-factor identification. Records of access

protocol issuance must be securely maintained. Auditor will seek evidence of adherence to policies and procedures.

Noting in particular, "*strong passwords, biometric identification, and/or multi-factor identification. Records of access protocol issuance must be securely maintained. ".* Storing password information in an encrypted vault is likely one component but does not cover strong password requirements nor records of access protocol issuance. Examples of how this might be achieved may include, but are not limited to, a process for documenting and tracking requests for access at the time of on-boarding and off-boarding both new employees and new client users. Additionally, illustrating your method of tracking and logging changes to access throughout an individual's employment or for a client user would be required as well.

In summary, Clause 1.6 is interested in what you are doing to ensure that proper controls are in place around your granting of access to consumer data to either your staff or your client users as well as storage of such user/password information.

Thank you for submitting your inquiry and giving the BSCC an opportunity to review. We believe we have responded fully to your inquiry. Please let us know if you have any further questions.

Issued June 2018
Revised July 2022
Reviewed August 2023