The Background Screening Credentialing Council

ACCREDITATION TIP

The Background Screening Credentialing Council (BSCC) has drafted the following accreditation tip for the US Employment Screening / General Background Screening BSOAP Standard, this tip 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 Tip, and to ensure our response applies to both Standards, the terms Organization and CRA may both be used.

TITLE: Clause 1.2 – Information Security Policy

Clause: Organization / CRA must have and follow a written information security policy which, at a minimum, complies with applicable law and regulation. Organization / CRA must designate one or more individuals responsible for implementing, managing and enforcing the information security policy (individual(s) may be internal or contracted).

A **Non-Conformity** for section 1.2 may look something like the following:

> "Testing of the control activity disclosed that the entity did not have an executed service level agreement in place with the third-party managed services provider they are contracted with. The vendor provides managed services that includes, but is not limited to, setting up new users, workstations, and regular maintenance on the entity's firewall. The entity categorized the managed services vendor as an "as needed" service provider."

The Audit Criteria for Clause 1.2 provides:

This is an overarching information security policy which broadly addresses security within the Organization environment. This policy may reference other security policies and/or procedures dealing with specific security topics. Such document(s) must, at a minimum, address: 1) key personnel, roles and responsibilities, 2) policy changes and modifications, 3) system configuration, 4) anti-virus, firewall, and router configuration, 5) data and information classification, 6) encryption, 7) access control, 8) electronic data retention, storage, and disposal, 9) paper and hard data retention, storage, and disposal, 10) data device retention, storage, and disposal, 11) incident response, 12) physical security, and 13) security policy revision history, and 14) Remote Workforce Policy. Auditor will seek evidence of adherence to policy.

We hope the above provides further information and clarification on the information provided in the Standard and may be used to improve your accreditation submission.

December 2018
Reviewed August 2023