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 1.4 - Intrusion and Data Security

Clause: Organization / CRA must have and follow procedures to prevent, detect, investigate and respond to an information system intrusion, including consumer notification and other breach notifications where mandated. At a minimum, procedures must meet all applicable legal and regulatory requirements.

A **Non-Conformity** sometimes identified for this clause is the absence of procedures and tools in place to prevent, detect, investigate and respond to an information system intrusion.

As is detailed in the Measure & Documentation Typically Subject to Desk Audit and the Potential Verification for Onsite Audit columns associated with this Clause, the Organization / CRA must be able to produce procedures (including evidence of adherence to the same) for preventing, detecting, identifying and responding to information system intrusions, including consumer notice and other breach notice requirements.

The Audit Criteria for Clause 1.4, provides:

> *Organization / CRA must present proof of tools used to protect network, data, and consumer information. This may be third-party audit results, intrusion/detection testing results, firewall protections used, website security, or other recognized security protocols and devices. Auditor will seek evidence of adherence to policies and procedures.*
>
> *Process/procedure must include [sic] but is not limited to: 1) individual to contact in case of intrusion and his/her back-ups, 2) necessity of immediately stopping intrusion activity, if still occurring, 3) determination of notification requirements, 4) preparing notification/s, 5) obtaining necessary approvals of notification language, 6) communicating notification, and 7) de-brief to prevent future occurrences. Auditor will seek evidence of adherence to policies and procedures.*

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.

November 2018
Reviewed August 2023