Information Sensitivity Policy and Procedure

Authorized By:	**Bryan Chapman**	**Date Authorized:**	**3/16/2011**
Effective Date:	**4/1/2011**	**Last Amendment Date:**	**11/3/2020**
Version Number:	**3**	**Document Number:**	**PR-INT-CD-4009**

Implementation & Review:	**Bryan Chapman, CEO**
Superseded Document:	
Related Documents:	

Any questions or concerns with this Policy and Procedure document should be referred to the first-line supervisor. If questions are not resolved, follow the organizational chart.

1.0 Purpose

The Information Sensitivity Policy and Procedure is intended to help employees of AboveTraining Inc. (dba StateFoodSafety) determine which types of information can be disclosed without authorization.

2.0 Scope

The kinds of information covered in these guidelines includes information that is either stored, shared, or collected via any means, such as user-provided information, client-provided information, PII, StateFoodSafety internal documents, and information that is shared electronically, on paper, orally, or visually. This policy also describes the procedure for verifying the identity of users for the purposes of program/exam security and PII protection.

3.0 Definitions and Descriptions

3.1 Definitions

- **"User"** is intended to mean a StateFoodSafety end user who may disclose personally identifiable information about him/herself during the registration and/or learning process.
- **"Client"** refers to enterprise or regulatory customers who may disclose information about their organization.
- **"PII"** or "Personally Identifiable Information" is information that is unique to an individual and may be used to identify or impersonate a user.

3.2 Descriptions

At StateFoodSafety, information is categorized into two main classifications:

- Public
- Confidential

Public information is information that has been declared public knowledge by someone with the authority to do so, is within the public domain, and can freely be given to anyone without any possible damage to StateFoodSafety, its users, or its clients.

Confidential information includes all other information and should be closely protected. Confidential information can include, but is not limited to:

- Trade secrets;
- Intellectual property, such as training, assessment, and software programs;
- Potential acquisition targets;
- User PII including, but not limited to:
    - Date of birth,
    - Phone numbers,
    - Physical address,
    - Driver license information,
    - Social security number,
    - Training and assessment outcomes, etc.;
- Client information;
- Third party confidential information, such as that identified in a non-disclosure agreement;
- Other information integral to StateFoodSafety's success.

4.0 Policy

Confidential information should not be shared between StateFoodSafety employees or with non-employees unless pertinent information is required by an employee to perform a legitimate job function or to fulfill a contract with a client.

StateFoodSafety employees shall use good judgment to secure confidential information within all reasonable means. When in doubt, an employee should assume the information is confidential and obtain clarification from a member of management council or senior management.

At all times, employees are governed by the StateFoodSafety Confidentiality Agreement, which all employees must sign as a prerequisite of their employment.

5.0 Procedure

Each user has a unique username and password for their exclusive use. During the checkout process, users must agree to StateFoodSafety's terms and conditions, which specify that login information may not be shared with or provided to other agencies, organizations, businesses, or individuals. Users are responsible for maintaining the confidentiality of their usernames and passwords.

For the purposes of PII and program/assessment security, if a user requires customer service after registering for training or assessment, StateFoodSafety customer service representatives must confirm the user's identity. This can be accomplished by asking the user to repeat or confirm PII that has been previously provided to StateFoodSafety during the purchase or registration process. StateFoodSafety customer service representatives cannot prompt or assist individuals in answering verification questions, as these actions can compromise confidential information, user

accounts, programs, and assessments. The user must be able to confirm his or her identity without assistance.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Revision History

October 2, 2020: Significant edits for brevity, clarity, and to include types of PII that should be considered confidential.

November 3, 2020: Amended to include clarity on procedure for verifying user identity.