****

#3 Information and Data Privacy

| **Assessment****Procedure****Number** | **ALTA Best Practices Framework: Assessment Procedures** | Assessment Recap |
| --- | --- | --- |
|  | **ALTA Best Practice 3.****Adopt and maintain a written privacy and information security plan to protect Non-public Personal Information as required by local, state and federal law.** | ***Overall Assessment Recap: If any individual procedure marked with an asterisk FAILS, Best Practice 3 FAILS.*** |
| 3.01\* | Obtain the Company’s information security program/policy to protect its Non-public Personal Information and verify that the program/policy is reviewed and updated at least annually, as necessary. | PASS / FAILIf no written procedures, Procedure 3.01 FAILS. |
| 3.02\* | Select a sample of 25 employees who have access to Non-public Personal Information (or 100% if fewer than 25 employees). Obtain evidence that they were trained in the Company’s information security program/policy to protect Non-public Personal Information.  | PASS / FAILIf 20% or more of items tested FAIL, Procedure 3.02 FAILS |
| 3.03\* | Obtain the Information Security Risk Assessment, including the risk ranking of information systems.Review the Company’s process for assessing risk to its customer information and verify that it includes the following:1. Locations, systems, and methods for storing, processing, transmitting, and disposing of its customer information.
2. Potential internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of Non-public Personal Information or customer information systems and assessments of the likelihood and potential damage to the Company and its customers of these threats.
 | PASS / FAILIf no written Information Security Risk Assessment, Procedure 3.03 FAILS. |
| 3.04\* | Verify that key controls, systems and procedures of the information security program are regularly tested by qualified independent staff in accordance with the risk assessment.Specifically, review that the following are included in the testing:1. Management’s documented approach for testing the information security program and evidence of testing.
2. Frequency of testing of the information security program.
3. Documentation of approach for tracking and remediating exceptions and/or control gaps.
 | PASS / FAIL  |
| 3.05\* | Verify employees are required to complete an acceptable use of information technology assets agreement at least annually (e.g., acceptable use of the Internet, email, and Company information resources). For the sample of employees tested in Assessment Procedure 3.02 above, review the signed Acceptable Use Policy.  | PASS / FAILIf 20% or more of items tested FAIL, Procedure 3.05 FAILS  |
| 3.06\* | Obtain and review written policies and procedures to verify logical access to information systems (i.e., network, data base, and application layers) containing Non-public Personal Information is restricted to authorized persons only. | PASS / FAILIf no written procedures, Procedure 3.06 FAILS. |
| 3.07\* | 1. For the sample of employees tested in Assessment Procedure 3.02 above, test the user access provisioning process to determine if access is approved in accordance with policy prior to granting.
	* Obtain evidence (invoice/documentation in personnel files, etc.) that 5 year Background Checks were conducted upon hiring or within the past 3 years.
2. Select a sample of 5 terminated employees or 100% if less than 5 within the assessment period.
	* Verify the user access de-provisioning process to determine if access for terminated employees was removed per policy.
3. Verify administrative access rights (i.e., ability to add, modify and remove user access) to systems containing Non-public Personal Information are not assigned to personnel performing business transactions within the system.
4. Verify access review is being performed by management at least annually to confirm that only required employees have access to customer information or customer information systems necessary to perform job functions.
5. Verify that logical access controls (e.g., unique User ID’s, complex passwords, etc.) to the network and information systems containing Non-public Personal Information are in place.
	* Obtain listing of user ID’s for systems with Non-public Personal Information. Verify ID’s are unique and assigned to specific users.
	* Test password configuration controls in accordance with policy.
 | If 20% of sub-procedures 3.07.a or 3.07.b FAIL, the sub-procedure FAILSIf sub-procedure 3.07.c, 3.07.d, or 3.07.e FAIL, the applicable sub-procedure FAILSOverallIf any individual sub-procedure FAILS, Procedure 3.07 FAILS  |
| 3.08\*  | 1. Review documented policies regarding the use of removable media (e.g., restricting the use of USB ports, CD/DVD writable drives, etc.).
2. Obtain evidence of system configuration settings demonstrating the restriction of removable media in accordance to policy.
 | PASS / FAILIf sub-procedure 3.08.b FAILS, Procedure 3.08 FAILS. If sub-procedure 3.08.a FAILS, but 3.08.b PASSES, then Procedure 3.08 PASSES. |
| 3.09\* | Inquire of management to determine if the Company:1. Provides encryption of electronically transmitted Non-public Personal Information.
2. Can provide evidence of system configuration settings demonstrating the use of encryption.
 | PASS / FAILIf sub-procedure 3.09.b FAILS, Procedure 3.09 FAILS. If 3.09.a FAILS, but 3.09.b PASSES, then Procedure 3.09 PASSES |
| 3.10\* | 1. Obtain and review documented procedures for monitoring, detecting attacks/intrusions into customer information systems, and responding to incidences. If monitoring of external threats has been outsourced, obtain evidence of reporting and subsequent management review.
2. Obtain a sample of 5 or 10%, whichever is greater, of notifications of security alerts (maximum of 25) and verify management’s follow-up activity.
3. Obtain and review documented procedures for security breach notification, including evidence of program review at least annually.
 | PASS / FAILIf no written procedures, Procedure 3.10 FAILS.If any individual sub-procedure FAILS, Procedure 3.10 FAILS.  |
| 3.11\* | 1. Verify access to physical locations containing customer information, such as buildings, computer facilities and record storage facilities, is limited to authorized personnel only. Inspect physical locations to verify that they are secured and access is limited to authorized personnel.
2. Obtain and review the Clean Desk Policy and verify compliance through inspection.
 | PASS / FAILIf any individual sub-procedure FAILS, Procedure 3.11 FAILS. |
| 3.12\* | 1. Obtain and review change management procedures when technology and business function changes are made.
2. Verify procedures are in place to determine that systems modifications (hardware and software) are consistent with the approved security program. Specifically, test a sample of 5 or 10%, whichever is greater (maximum 25) of hardware or software changes to verify that they are documented, tested and approved.
 | PASS / FAILIf sub-procedure 3.12.b FAILS, Procedure 3.12 FAILS. If sub-procedure 3.12.a FAILS, but 3.12.b PASSES, then Procedure 3.12 PASSES  |
| 3.13\* | Obtain management’s procedure for data and system backup and business resumption to protect against destruction, loss, or damage of information from potential environmental hazards, such as fire and water damage or technological failures.  | PASS / FAIL  |
| 3.14\* | Determine whether the Company provides Non-public Personal Information to any other party or whether any other party has access to Non-public Personal Information through service provided directly to the Company.1. Verify and obtain evidence that Company conducted due diligence in selecting its service providers and taking information security into consideration.
2. Verify that Company has controls to monitor security procedures of service providers to safeguard customer information (i.e. review the results of audits, security reviews or tests, intrusion logs, or other evaluations).
 | PASS / FAILIf any individual sub-procedure FAILS, Procedure 3.14 FAILS.  |
| 3.15\* | Verify whether Company provides Privacy Policy to customers. Obtain and inspect evidence of notification using the same sample as in Assessment Procedure 2.06 above. | PASS / FAILIf 20% or more of items tested FAIL, Procedure 3.15 FAILS  |
| 3.16\* | Determine through inquiry of management whether the Company maintains a website. If so, inspect the Company's website and verify the following: 1. The website includes a privacy statement.
2. The website's privacy statement accurately discloses what Non-public Personal Information is obtained on the site.
 | PASS / FAILIf any individual sub-procedure FAILS, Procedure 3.16 FAILS. |
| 3.17\* | 1. Obtain and inspect policies and procedures over record retention and disposal. Verify procedures are in place for disposal of Non-public Personal Information.
2. If document/electronic media disposal services are provided by a third party, obtain evidence of the contract agreement/SLA and a recent document disposal certificate from the vendor.
 | PASS / FAILIf any individual sub-procedure FAILS, Procedure 3.17 FAILS. |