ACCEPTABLE USE POLICY AUDIT Of

Our Company, Inc.

**December 1, 2015**

James Levan

Anthony Lucas

Alaa Abuali

Vinh Nguyen

**Audit Objective**

The primary purpose of the audit is to assess the effectiveness and efficiency of the Acceptable Use Policy by ensuring that internal controls are established, properly documented, maintained and adhered to.

**Scope and Approach**

These internal controls are designed to provide reasonable assurance regarding the safeguarding of resources, reliability of operating and financial information, and compliance with regulations and policies established by law and “Our Company”. The process will include review of operational behaviors, development of control procedures and policies, communication, and log monitoring.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy** | **Policy Goals** | **Control****Objectives** | **Control****Activities** | **EVIDENCE** |
| **Password/Security Access** Revision History:10/07/2015 – Initial10/30/2015 – Update, included Cell Phones, Tablets and Laptops11/15/2015 – Update to include use of cloud based storage | Defines minimum and maximum length of passwords, password complexity, how often it must be changed | Computer access controls include protecting the integrity and accuracy of data and applications providing for the security of confidential and proprietary informationOr data.  | Password must meet complexity requirements-use of numerical, capital & Symbol | User Policy and Procedure |
| Access privileges granted to appropriate personnel | System user listing and job role report (SACL) |
| Account Lockout after 3 failed attempts | Testing results documentation |
| Removal or deactivation of passwords upon leave or termination of employee | Audit logging enabled to log any unauthorized access |
| **Data Classification Policy**Revision History10/07/2015 – Initial10/30/2015 – Update, included Cell Phones, Tablets and Laptops11/15/2015 – Update to include use of cloud based storage | Allows users to understand, manage, and employ an appropriate level of security for the data. | Establish data security definitions for legal/regulatory compliance, data will be classified the appropriate access category. | All company documents are systematically classified into categories based on the sensitivity of information. | Our Company’s Data Classification Policies |
| All data classes have required length of storage and are automatically deleted if information is not required by legal reasons. | Vendor’s Data Classification Policies |
| Stratified random sample of data classified as public, sensitive, proprietary, confidential, and restricted. | Judgmental review of data storage length of categorized data |
| **Asset Control Policy**Revision History10/07/2015 – Initial10/30/2015 – Update, included Cell Phones, Tablets and Laptops11/15/2015 – Update to include use of cloud based storage11/15/2015 – Clarified policy language to be more consistent with regulatory standards | Asset tracking so the location of all computer equipment is known, network administrators will know which assigned user and computer is in use  and that data on a computer may be sensitive and must be encrypted | Ensure company owned devices/hardware and work related devices are accounted for during their entire useful life and properly disposed of afterwards to ensure confidentiality, integrity, and availability of data. | System must be locked or logged out when unattended | Asset Control Policy |
| Data Security will have authority to deny any device access to systems when they deem that such device does not provide adequate security. | Field-test of vendor remote access deletion software and encryption. |
| Remote Access Deletion Software is installed on all company laptops for deletion of sensitive data of lost or stolen laptops. | Review KPI of lost equipment data to length of time of company response and course of action. |
|  |  |
| **Social Media Policy**Revision History10/07/2015 – Initial10/30/2015 – Update, included Cell Phones, Tablets and Laptops11/15/2015 – Update to include use of cloud based storage | Defines the parameters of proper social media usage by employees and ensures that opinions and legal liability of employee created social media content is not of the opinion of Our Company. | To ensure that Our Company goodwill and reputation is maintained in the highest regard and is not falsely represented by individual employees. | When discussing or sharing information about the Company, identify yourself as an employee | Disclaimer such as "The posting on this site are my own and do not reflect the views of the Company." Is in place. |
| Maintain the confidentiality of proprietary, trade secrets, sensitive, or confidential information, internal reports, policies, or procedures  | Random sampling done on employees that are active on social media. |

**Document Requests**

1. User Access & Acceptable Use Policy
	1. Authentication Policy
	2. Active Directory Computer Reports
	3. System Access Control List (SACL)
	4. User Access Forms
	5. List of Current Active Users
2. Data Classification Policy
	1. Vendor’s Data Classification Policy
3. Asset Control Policy
	1. List of known company assets/hardware lost
	2. List of reported company asset/hardware lost

**Test Steps**

1. Obtain proper documentation of User Access & Acceptable Use Policy, Data Classification Policy, Asset Control Policy and all other related documents.
2. Review current policies to ensure sufficiency and understandability.
3. Interview employees to ascertain employee understanding of said policies.
4. Conduct a sample audit test of key policy functions and record Key Performance Indicators (KPI).
5. Review KPI and compare with results of last audit.