IT Governance
Policy Project
October 9, 2015

Yizhou An
Jiehong Huang
Blake Koen
Anh Tran
Shizhong Yang

Policy Department
Social Security Number Policy
ABC Company
October 9, 2015

1. Objectives:

During the course of our day-to-day operations, we will have to collect Social Security Numbers in order to establish accounts and complete day-to-day operations. We understand that this is very sensitive information and we will take reasonable steps to ensure the security of our customers' personal information. The purpose of this policy is to create awareness of the policy and to ensure that there are procedures in place so that this information stays private. Failure to do so can result in fines, penalties, legal and corrective fees as well as damage to our reputation. Therefore, everyone must follow our policy.

2. Social Security Number:

Social Security number is a unique 9-digit identification that are issued by the U.S government to each individual U.S citizens, permanent residents, and temporary residents.

3. Roles and Responsibilities: The Information Technology Department will create or install software and hardware. The Information Security Department will monitor the systems for irregularities and will report unauthorized social security number access to

the Legal department and Human Resources for disciplinary action, if any. Access to sensitive information is based on job function. Access can only be requested by an employee's supervisor and not the employee themselves. If the employee only needs access on a limited basis, access shall be removed when access is no longer necessary.

4. Scope:

This policy applies to all employees, contractors, and vendors who, in the course of employment or duties on behalf of the company, have access to Social Security Numbers.

5. Policy:

5.1 Personnel Controls: All of our employees will be properly screened to ensure that they can do the job and to ensure that there is no reasonable reason for us to suspect that they will do anything that puts our customers information at risk. All employees will be properly supervised and a segregation of duties will be established. Personnel with access to sensitive information are required to take two weeks of vacation each year (minimum of one week at a time). Third party contractors are required to follow the same controls as internal employees.

5.2 Access Controls: In addition to our password policies, we have strict access controls. Access is based on job descriptions and employees may not access any data that is not relevant to their job. Any employee that has left the organization, whether they quit or were fired, will immediately have all of their access revoked. Employees cannot access our network outside of the office without special permissions. We require our customers to create strong passwords. The Passwords must include a mix of lower and upper case letters and at least one symbol. We require that our customer passwords are at least 8

characters. Our internal passwords require the same controls and in addition they must be changed every 60 days. Social security numbers may not be used as passwords.

5.3 Email and Mail: Social Security Numbers are not permitted to be printed/appear in whole on outgoing E-mail/Mail. If it is necessary to include a Social Security Numbers than only the last four digit of the Social Security Numbers may be visible.

5.4 Account Verification: Employees may only ask for the last 4 digits of a Social Security number for verification purposes.

5.5 Disposal: Any paper or equipment containing social security numbers will be disposed of in a secure manner.

5.6 Maintaining the Security and Privacy of Social Security Numbers

5.6.1 Data Security: All data is encrypted and stored behind a secure firewall. Any changes to the Information systems will not take place without proper testing to ensure that the sensitive information remains secure. Virus software is maintained and is up to date. In addition, no Social Security Numbers will be kept on anyway outward facing servers.

5.6.2 Technology Standards: A configuration map and a current technology inventory shall be kept at all times. This will help us to know exactly all of the devices that store Social Security Numbers and let us know who has access to them.

5.6.3 Process: Workflows will demonstrate how departments work together to ensure privacy.

5.6.4 Testing: We will have an instruction manual for employees to perform tasks that will ensure that our Social Security Policy is working as planned.

6. Security and Enforcement:

6.1 Physical security: All of our buildings are monitored by 24-hour video surveillance. Branch locations will only be open during business hours when reasonable levels of staff are in place. Our data centers and back office buildings require key card access to enter the building and to enter specific departments, and have 24-hour security patrols.

6.2 Violations: Violation of this policy is unacceptable and employees that violate this policy may be subject to disciplinary action.

First offence: The employee will meet with their supervisor to review their actions and may be subject to disciplinary action.

Second offence: Will be brought under a committee to oversee the hearing and may be subject to disciplinary action.

Third offence: Will be subject to disciplinary action.

Disciplinary action may include a formal write up, suspension, or termination of employment.

7. Review Schedule:

We take every effort to ensure that the policy is working and is up to date with current technologies. Therefore the policy will be reviewed at least once a year, and will be reviewed if there is a breach, or a change in regulatory laws. The policy may also be reviewed as new technology is introduced. Changes should include input from end users and senior management.

Employees will be notified of changes via e-mail.

8. Policy History:

Policy implemented October 2015