

**Social Security Number Policy**

Document Title: SOCIAL SECURITY NUMBER POLICY

Version Control Number: ISMS-SSN 2017-1.0

Created and maintained by the Chief Information Security Officer

Approved by IT Steering Committee on September 28, 2017

Published on October 2, 2017

**Objective:**

As part of its day-to-day business operations, the ITACS Credit Union maintains, stores, processes, and exchanges sensitive information related to its members and employees. As a result, ITACS is required by various laws, regulations, and business agreements (e.g**.,** Gramm-Leach-Bliley Act (GLBA), National Credit Union Association (NCUA), Health Insurance Portability and Accountability Act (HIPAA)) to protect such information.

These regulations and laws require ITACS to protect member and employee social security numbers from unauthorized access, disclosure and destruction. When information does require protection, the protection must be consistent. Preventive controls are applied to data stored in ITACS core system, corporate databases, and server environment. Whether stored in a database, cloud storage, workstation, file cabinet, desk drawer, garbage can, or in the mail, social security numbers must be subject to appropriate and consistent protection.

The objective of the Social Security Number Policy is to provide guidance to the ITACS user community on handling of member and employee social security numbers and the controls needed to protect this information.

**Scope:**

All officials, employees, contractors, part-time and temporary workers, and those employed by others to perform work on ITACS premises, or who have been granted access to its information or systems, are covered by this operational policy and must comply with all associated standards and guidelines. Hereafter, the scope of this policy will be referenced as Users.

**Policy Statement:**

In performing required job functions, users may access social security numbers. Any access to social security numbers that falls out of the context of required job functions as documented in formal job descriptions or statements of work are prohibited.

**Roles and Responsibilities:**

ITACS Senior Management has adopted this Social Security Number Policy to accomplish the objectives and principles expressed within the Information Security Policy. The Chief Information Security Officer maintains the *Social Security Number Policy*. Questions or concerns about the implementation of this policy should be referred to the Chief Information Security Officer by email or phone.

ITACS management, including senior management and department managers, is accountable for ensuring that the *Social Security Number Policy* is properly communicated and understood within their respective departments and with contracted third-party vendors. This policy should be read in conjunction with all other applicable corporate policies (e.g., the Information Security Policy, Acceptable Use Policy and the Clean Desk Policy, etc.)

Management also is responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the *Social Security Number Policy*.

All users identified in the scope must familiarize themselves with and adhere to this operational policy.

Any violations to this policy will be investigated by the Chief Information Security Officer. Investigation results will be shared with Human Resources. Violations of this policy may result in disciplinary action, up to and including termination.

**Policy Non-Compliance, Misuse, or Abuse Reporting**

*Any actual or suspected information security incident* that affects the confidentiality, integrity, and availability of ITACS’s information in any form (e.g., paper, electronic), IT infrastructure, or electronic communications systems *must be reported immediately to the Chief Information Security Officer*.

This may include, but is not limited to: (1) unauthorized access, use, change, destruction, disclosure, or loss of any social security number(s); (2) improper use, destruction, disposal, loss, theft, or compromise of ITACS’s IT infrastructure or electronic communication systems.

Additionally, users must immediately report any observed or suspected information security weakness in systems, processes, or services to the Chief Information Security Officer.

**Review and Record of Revision:**

The Social Security Number Policy will be reviewed periodically by the Chief Information Security Officer, and any changes will be submitted to the IT Steering Committee for approval.

|  |
| --- |
| **Revision Record** |
| **DCN** | **Date** | **Description of Change** | **Revised By** |
| ISMS-SSN 2017-1.0 | September 26, 2017 | Initial document | Chief Information Security Officer |
|  |  |  |  |

|  |
| --- |
| **Approvals** |
| **DCN** | **Approved By** | **Date** |
| ISMS-SSN 2017-1.0 | IT Steering Committee – Michael Gibbons  | October 2, 2017 |
|  |  |  |

**Terms & Definitions**

*Availability* The property of information being accessible and usable upon demand by an authorized entity.

*Confidentiality* The property that information is not made available or disclosed

to unauthorized individuals, entities, or processes.

*Electronic Communications* All ITACS information systems and equipment, including

*Systems* but not limited to, the Internet, Intranet, e-mail, servers, workstations, laptops, printers, copiers, fax machines, telephones, and mobile devices.

*Information Asset* Any information regardless of its form (e.g., electronic, physical,

verbal) that has value to the organization and that is created, used, shared, stored, or disposed of by ITACS or its affiliates in support of its business processes, including all information maintained or accessed through systems owned or administered by or on behalf of the Credit Union. Assets also include the IT infrastructure mentioned above.

*Information Security Incident* Unauthorized access, use, change, destruction, or disclosure of

sensitive company, member, or employee information; a compromise of ITACS’s IT infrastructure that may affect its confidentiality, integrity, or availability.

*Integrity* The property of safeguarding the consistency, accuracy, and completeness of information assets.

*Official* Any member of ITACS’s Board of Directors and/or members of Committees appointed by the Board of Directors.

*ITACS User* Any individuals, groups, or organizations (e.g., officials, employees, and contractors) who have been granted access to ITACS’s information or systems in order to perform a prescribed business or operational function of the Credit Union.

**Related Policies, Standards, and Processes:**

* Acceptable Use Policy
* Administrative Control Policy
* Badge Access Policy
* Data Retention Policy
* Firewall Policy
* Information Security Policy
* Logical Access Policy

**Appendix A: Controls around Social Security Numbers**

Consider the business need and legal requirements for using Social Security Numbers. Use alternative methods of identification when possible such as Employee ID number, Customer ID number etc.

Data Masking

* If a business need is identified that requires the use of Social Security Numbers, consider masking part of the number (e.g. last four digits XXX-XX-1234)

Data at Rest

* Social Security Numbers must be encrypted at rest using Advanced Encryption Standard (AES) with 256-bit keys and be Federal Information Processing Standard (FIPS) 140-2 compliant.

Portable Storage Devices

* Storage of Social Security Numbers on portable storage devices (USB flash drives, portable hard drives, etc.) is prohibited. All user machines are configured to only permit keyboard, mouse and speaker functionality. All other peripherals are prohibited unless a formal documented exception is granted by the Chief Information Security Officer with an approved business justification.

Retention Schedule

* For documents containing Social Security Numbers, if it is not required to retain the document for future use, securely destroy the documents as soon as possible. If it is determined that storage of documents containing Social Security numbers is necessary, do so in a manner that will adhere to the aforementioned data storage controls. Do not keep copies of official documents which are being retained by another department (e.g. employee W-2 forms should only be kept by the Payroll department.)

Data in Transit

* Social Security Numbers must be encrypted during transit using SSL/TLS connections with a 2048 bit key.

Email

* Whenever possible, avoid sending documents containing Social Security Numbers via email. If possible, deliver the documentation personally.

Fax

* Documents with Social Security Numbers should only be Faxed to known parties where access to the fax machine is limited and protected. If Faxing sensitive information is required, use the following guidelines:
* Notify the recipient in advance that sensitive data is being transmitted
* Indicate on the FAX cover sheet that the materials are confidential
* Confirm the FAX has been received

Clean Desk Policy

* When dealing with sensitive information, employees are required to store all printed documents containing sensitive information in locked filing cabinets. Users are prohibited from removing sensitive information in physical form (paper) from company premises. Periodic reviews will be performed to look for unattended documents containing sensitive information as well as unlocked storage.

System monitoring

* On a regular basis we will perform system monitoring to confirm proper usage and functioning of software. This is a part of an overall audit to confirm an appropriate control environment. Modeling tools will be utilized to predict potential system failures based on past failures, usages trends, and management expectations of new users. The databases that house PII including social security numbers will be part of the daily monitoring process to confirm protections, functionality and performance.

 Access logs

* Will be utilized to store sufficient chronological information in operations logs to enable the review and examination of the time sequences of operations. This will help determine the potential unauthorized access to social security numbers.

Video Camera

* Will be recording at all times to review physical access to the premises. The data will be recorded and backed up on a separate server. This information will be accessed if a breach of social security numbers occurs.

Antivirus Software

* Antivirus software will be implemented to maintain preventive, detective and corrective measures especially up-to-date security patches and virus control. This will help protect social security numbers from viruses, worms, spyware, and spam.

Firewall

* There will be network filtering mechanisms in the form of a firewall to monitor and control inbound/outbound traffic to protect the release of social security numbers.

Email Gateway

* An email gateway will be implemented to keep out unwanted content in email messages such as malware, phishing attacks and spam. The email gateway will also detect and block the transition of sensitive data such as social security numbers.

Internet Proxy Server

* To protect social security numbers, we will implement a reverse proxy server. This will hide the existence of characteristics of an origin server which will make it difficult to access sensitive information.

**Appendix B: Incident Response**

The ITACS Credit Union is committed to safeguarding Personally Identifiable Information (PII) and implementing sound procedures for handling incidents in accordance with federal and state statutes and regulations.

Social Security numbers are considered sensitive PII since they can be used to distinguish or trace an individual’s identity and could result in substantial harm if lost, compromised, or disclosed without authorization. A PII incident includes, but is not limited to, the unintentional or intentional loss of information, or unauthorized access, acquisition, modification or disclosure of PII information.

**Computer Incident Response Team**

The Computer Incident Response Team (CIRT) is the group of selected employees who are responsible to promptly and correctly handle an incident. The objective of the CIRT is to quickly contain, investigate, and recover from an incident involving information systems.

**System Steward**

The System Steward is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

**CIRT Members**

The CIRT is comprised of an employee from the following departments. All members of the team will be approved by the CISO. Once the team is assembled a list of the employee’s name, email, and business phone number should be made readily available to all members of the organization.

* Executive Management
* Information Security (IT Security)
* IT Management
* IT Auditor
* Security
* Legal
* Human Resources
* Financial Auditor

**Incident Response Process**

The incident response process is initiated with a suspected breach of unencrypted electronic restricted data. As soon as the System Steward becomes aware that a suspected security breach involves a system containing electronic restricted data, it will notify IT Security no later than 24 hours after becoming aware of the suspected breach. Upon receipt of this notification, IT Security will send an alert to the CIRT and file an initial incident report. The System Steward may also file a police report if criminal activity is suspected.

IT Security and the appropriate parties must work together to disable unauthorized access to restricted data where applicable and restore the service and integrity of the system with appropriate documentation and preservation of evidence.

Upon resolution of the breach, the CIRT will submit a final incident report to the CISO.

**Notification Procedures**

If unencrypted electronic Social Security Numbers are believed to have been acquired by an unauthorized party, all affected subjects must be notified. Law enforcement must be consulted to ensure that notification will not impede a criminal investigation.

Where applicable, notification will inform affected subjects about free credit protection services such as annual credit reports and credit fraud alerts. Under certain circumstances credit monitoring services may be offered to individuals who are affected by the breach.

**Lessons Learned**

After the incident is resolved, the CIRT will review and evaluate how the incident was handled. The information gathered will be used to improve on the incident response process for future incidents. The data gathered will also aid in future policy and procedure developments and revisions as needed.

**Appendix C: Social Security Number Policy - User Agreement**

I agree that I have read this document in full and understand the acceptable use and my responsibilities as a user entrusted with confidential information. I agree to these terms in their entirety and agree to fully and to the best of my abilities comply at all times. I fully understand and have accepted the contents of this version of the policy under no coercion from my employer. I understand that violations to this policy can result in disciplinary actions, up to and including termination of employment. I further understand that ITACS Credit Union can, at any time and at its discretion, modify and provide me an updated copy of this policy which will require my understanding and agreement at that time.

**Employee Name (printed): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Employee Signature (printed): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**HR Use Only:**

**HR Acknowledgement (initialed by HR Admin): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Employee Manager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Employee Department: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**