# POLICY MEMORANDUM

| | | | |
|---|---|---|---|
| Branch | General Counsel | Number | 16-057 |
| Division | Information Security Office | Effective Date | 3/15/17 |

**Title** Internet Usage Policy

**Policy** It is the policy of CalSTRS to provide internet access to California State Teachers' Retirement System (CalSTRS) employees and contractors as needed to support the business goals and objectives of CalSTRS. Violation may result in access to internet services being revoked without notice and depending on the violation, may lead to corrective action, dismissal or criminal prosecution.

**Standard** The internet is to be used as part of the normal execution of job responsibilities. All users are expected to use the internet responsibly and exercise good judgement to protect CalSTRS information and assets. Users may make incidental use of the CalSTRS internet facilities for personal activities, provided that such activity is kept to a minimum as defined by the users' manager, is limited to the employee's or contractor's own time, and does not interfere with job performance, adversely affect the morale or performance of co-workers, or detract from the professional image of the office. Personal use is prohibited if it is related to any activity considered inconsistent with CalSTRS Policies.

**Requirements** All CalSTRS employees and contractors are required to read the CalSTRS Internet Usage Policy and must sign the CalSTRS Internet Usage Acknowledgment form (ISO 1950) when they start work with CalSTRS and annually thereafter.

***CalSTRS Security Controls***

CalSTRS reserves the right to record and monitor internet usage for all users using any form of the CalSTRS network at any time and therefore, no internet user should have any expectation of privacy for their CalSTRS internet usage.

CalSTRS security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or email message, each internet endpoint, and each file transfer into and out of the CalSTRS network. CalSTRS reserves the right to inspect any and all files stored on any CalSTRS equipment in order to assure compliance with CalSTRS policies.

CalSTRS uses software and data to identify internet sites deemed offensive sexually explicit, or inappropriate and may block access from within the CalSTRS

network to all such known sites. Access to website(s) will be given only if the internet services and function serve a legitimate business purpose for CalSTRS. This can be requested through CalSTRS Request to Unblock a Web Site or Web Page form (ISO 1593).

CalSTRS systems or servers must not facilitate or connect to internet services unless the resource specifically requires the internet to perform its functions. In such event, the system or server will be granted the minimal level of internet privileges.

***Employee and Contractor User Conduct***

CalSTRS has installed a variety of firewalls and other security systems to ensure the safety and security of the CalSTRS network. No CalSTRS employee or contractor shall deliberately attempt to disable, defeat or circumvent any CalSTRS security facility.

The use of remote software tools are prohibited (i.e. TeamViewer, Virtual Network Computing, Join.me, etc.) unless an approved variance is on file.

CalSTRS employees or contractors accidentally connecting to a site that contains sexually explicit or offensive material must disconnect from that site immediately and must inform their manager or supervisor of the incident.

Users are prohibited from downloading and installing software from the internet. Downloaded software must be requested through the Service Desk and scanned for viruses before it is run or accessed.

Files containing confidential or sensitive data that are transferred in any way across the internet must use encryption to protect the confidentiality of the data. Those with a business need to transfer confidential or sensitive data across the internet must contact the Information Security Office to determine the most appropriate method for encryption and follow the Data Encryption Security Policy.

Under no circumstances will a CalSTRS employee or contractor use the CalSTRS internet facilities and computing resources to:

- Intentionally transmit or receive illegal or offensive materials (i.e., materials that are abusive, obscene, pornographic, profane, sexually oriented, promote racism/hate). In addition, illegal or offensive material may not be archived, stored, distributed, edited or recorded using CalSTRS resources.
- Download entertainment software or games, or to play games against opponents over the internet.
- Download or distribute pirated software, music or data.
- Download music or any other illegal downloads which infringe on copyright laws.

- Download and store non-business related files (i.e., audio, video, pictures, etc.) on CalSTRS devices including CalSTRS network drives in excess of the Enterprise Information Management's Individual Drive Storage Standard. Non-business files will be deleted (upon confirmation with the owner that files are non-business in nature).
- Deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- Disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- Partake in gambling activities.
- Access any personal web-based e-mail services (i.e., Gmail, Hotmail, Yahoo Mail, etc.)

## Exceptions

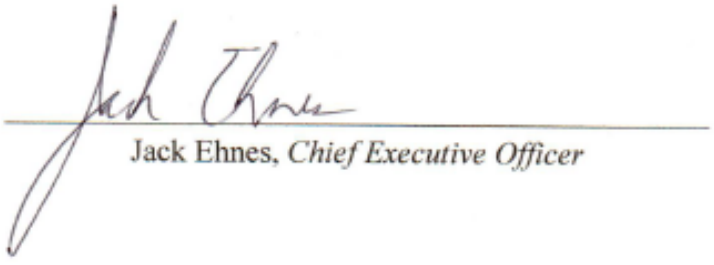
Requests for an exception must be submitted to the Information Security Office using the CalSTRS Variance Request form (ISO1801). If a standard cannot be met as stated in this document, an alternate solution may be proposed using the CalSTRS Variance Request form (ISO1801). A risk assessment will be conducted by the CalSTRS Information Security Office and a determination will be made if the exception is approved.

By designation from the Chief Executive Officer, the Chief Information Security Officer (CISO) has approval authority. The Information Security Office will analyze the risk and forward the request with a recommendation to the CISO for consideration.

## References

Government Code section 11549.3
State Administrative Manual section 5300 et seq.
CalSTRS Information Security Policy (#09-003)
CalSTRS Software Acquisition & Management Policy (#15-122)
CalSTRS Individual Drive Storage Standard (15-124)
CalSTRS Data Encryption Security Policy (09-004)
CalSTRS Confidentiality, Non-Disclosure and Acceptable Use Agreement (Form ISO 1949)

## Approved



Jack Ehnes, *Chief Executive Officer*