South Dakota Legislative IT Policy

— General —

Legislative Research Council

December 1, 2016

PENDING APPROVAL

SOUTH DAKOTA
LEGISLATURE
LEGISLATIVE RESEARCH COUNCIL

1 − Acceptable Use Policy

Purpose

The Legislative Research Council's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Legislature's established culture of openness, trust, and integrity. The LRC is committed to protecting the Legislature's users from illegal or damaging actions by persons, either knowingly or unknowingly while using LRC technology.

All legislative technology and systems are the property of the LRC. These are created and maintained in the interest of the South Dakota Legislature's duties.

Effective security is a team effort involving the participation and support of every user who deals with information or information systems. It is the responsibility of every user to know these guidelines and to conduct their activities accordingly.

Policy

General Use and Ownership
The Legislature's confidential and proprietary information stored on electronic and computing devices whether owned or leased by the Legislature, the user, or a third party remains the sole property of the Legislature.

Each user has the responsibility to promptly report the theft, loss or unauthorized disclosure of the Legislature's confidential and proprietary information.

Each user may access, use or share the Legislature's proprietary information only to the extent the user is authorized and is necessary to fulfil the user's assigned job duties. A user should not access legislative information that is not within the scope of the user's work.

Legislative technology (computers, internet, email, etc.) shall be used in an appropriate manner. As it applies to the legislative email system, emergency communications and reasonable and appropriate personal communications are allowed.

Under no circumstances are users allowed to use the legislature's technology to engage in outside business interests, inappropriate, or illegal activities. Abuse of the system is not acceptable. Users should not expect privacy or confidentiality when using state resources. Use common sense. If in doubt, do not use state resources. For security and network maintenance purposes, authorized persons within the Legislature may monitor equipment, systems, and network traffic at any time with prior approval from the Director or IT Manager.

Security and Proprietary Information
All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. It is recommended that each user lock the screen or log off when the device is unattended.

Users must exercise extreme caution when opening email attachments received from known and unknown senders, which may contain malware or other malicious content. Users should not forward suspicious emails or download attachments, but should inform Legislative Information Technology about the incident for further instructions.

Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions for their legitimate job responsibilities with approval from the Director or IT Manager.

The following lists is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

- Accessing data, a server, or an account for any purpose other than conducting the Legislature's business, even if the user has authorized access, is prohibited;
- Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.);
- Revealing a user account password to others or allowing unauthorized use of a user account by others. The account holder is responsible for the access granted to third parties;
- Making fraudulent offers of products, items, or services originating from any South Dakota Legislature account;
- Effecting security breaches or disruptions of network communication;
- Port scanning or security scanning is expressly prohibited unless prior notification to LRC IT is made;
- Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty;
- Circumventing user authentication or security of any host, network or account;
- Interfering with or denying service to any other user's device (for example, denial of service attack);
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet;
- Providing information about, or lists of, the Legislature's users to parties outside the Legislature without approval from the Director or Deputy Director; and
- Downloading or installing software unapproved by LRC IT.

Email and Communication Activities

When using legislative resources to access and use the internet, users must realize they represent the Legislature.

The following activities are prohibited:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to persons who did not specifically request such material (email spam);
- Unauthorized use, or forging, of email header information;
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies; and
- Unauthorized distribution of confidential legislative information.

2 – Password Policy

Purpose

The purpose of this guideline is to provide best practices for creating and protecting secure passwords. This guideline applies to all passwords. All users, including contractors and vendors with access to the Legislature systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Furthermore, this policy will establish a standard for the protection of those passwords and the frequency of change.

The scope of this policy includes all users, including contractors and vendors, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Legislature facility or cloud resource, that has access to the Legislature network, or stores any non-public legislative information.

Policy

Password Guidelines
All passwords should meet or exceed the following guidelines:

- Must contain at least 8 characters;
- Must contain two of the following three bullet items:
    - Contain both upper and lower case letters;
    - Contain at least one number (for example, 0-9); and
    - Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/);
- Must NOT contain your name;
- Passwords expire every 90 days;
- Cannot reuse the last five passwords; and
- Password reset enforced through server-side technologies.

Lockout
A lockout will occur after 5 failed attempts.

There will be a three-minute lockout period (can retry after three minutes).

If you are unable to gain access, contact LRC IT.

Password Protection
To ensure password protection:

- Do not share the Legislature passwords with anyone. All passwords are to be treated as sensitive, confidential legislative information;
- Passwords must not be inserted into email messages or other forms of electronic communication;
- Do not hint at the format of a password (for example, "my family name");
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption or password protection;
- Do not use the "Remember Password" feature of applications (for example, web browsers); and
- Any user suspecting that the user's password may have been compromised must report the incident and change all passwords.

3 – Email Policy

Purpose

Electronic email is used extensively in the Legislative and is often the primary communication method within the LRC. At the same time, misuse of email can pose many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications. This policy outlines the minimum requirements for use of email within the Legislature network and covers appropriate use of any email sent from a Legislature email address and applies to all users.

Policy

Users should have no expectation of privacy in anything they store, send or receive on the legislature's email system.

See LRC IT for assistance with sending confidential information.

Upon the departure of a user from the Legislature, email will be retained 30 days.

It is strongly advised that all users should refrain from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct South Dakota Legislative business.

Messages may be monitored with the approval of the director or IT manager in the course of providing reliable and secure email services. Reasons an email account may be monitored would be suspicion of SPAM, Viruses, Malware, or other threats that could compromise the mail server.

Legal Assistance
In the event of a subpoena or other legal action, the LRC IT team will work with authorities in providing subpoenaed records from the legislative email system. Requests to users for email correspondence outside of the Legislative email system are the responsibility of users and their third-party email provider to obtain.

4 – Personal Device Policy

Purpose

At the Legislature we acknowledge the importance of technology for communication and productivity. In addition to the increased use of personal devices, users have requested the option of connecting personal devices to Legislature's network and equipment. This policy provides guidelines for the use of personal devices. All users that access Legislature's technology, network, and/or services are bound by the conditions of this policy.

Policy

Personal devices may connect to the guest wireless network;

Support services are limited to:

- Guest internet connectivity;
- Configuration of legislative email; and
- Based on time availability, other services may be performed if they pertain to legislative business.

5 – Software Policy

Purpose

This policy provides guidelines for the installation and use of software on Legislature devices.

Policy

All non-standard software must be approved by LRC IT prior to installation to ensure:

- Purchase approval process is followed;
- Proper licensing;
- Compatible with our devices and network; and
- Does not pose a security risk to our infrastructure.

iOS users may utilize Apple Appstore apps using their judgement on appropriate use.

6 − Internet Usage Policy

Purpose

The purpose of this policy is to define the appropriate uses of the internet by legislators and employees. This applies to all users who access the internet through state-owned network resources.

Policy

Allowed Usage

The internet is an extremely useful tool in achieving the goals of the Legislature. Staff may use the internet to conduct official business or for personal, noncommercial, nonpolitical purposes on their personal time. Because a flat fee is paid by the state for all internet access, no additional costs are incurred through personal use of the internet. In addition, personal use of the internet offers staff an opportunity to develop skills and identify valuable internet resources. The public and the Legislature benefit by permitting staff to use their own time to enhance these skills. Disregard for the guidelines or other improper use of the internet may result in cancellation of a person's access or other discipline.

- Users have an obligation to utilize the internet in a responsible and informed manner, conforming to network etiquette, customs and courtesies;
- Users should identify themselves properly when using the internet, conduct themselves professionally realizing that they are viewed as representatives of the Legislature, and be aware that their activities reflect on the reputation and integrity of the Legislature;
- Each user is individually responsible for the content of any communication sent over or placed on the internet; and
- To protect against viruses, users should not download onto state-owned computers executable files or application software (including but not limited to utility software, freeware and shareware) without obtaining prior authorization from LRC IT.

Prohibited Usage

The following activities are prohibited:

- To access inappropriate websites;
- For any purpose that violates United States or South Dakota laws;
- To transmit or obtain threatening, obscene, harassing or malicious materials;
- To use abusive or objectionable language in either public or private messages;
- To misrepresent oneself or the Legislature; and
- For activities or uses that may cause congestion or disruption of networks or system including such activities as distribution of chain letters or unsolicited advertising.

LRC IT

Scott Darnall, Manager

Kevin Kumpf, Programmer/Analyst

Hilary Carruthers, Computer and Web Support Specialist

Brian DeBolt, Network Administrator

LRCHelpDesk@sdlegislature.gov