Privacy Expectations for SULC Computing Resources
Policy Number 8-0014

Responsible Unit: Information Technology	Effective Date: 5/7/2009
Responsible Official: Associate Vice Chancellor, Information Technology	Last Reviewed Date: 7/15/2019
Policy Classification: Information Technology	Origination Date: 5/7/2007

1.0 Rationale:

This policy seeks to facilitate teaching, research, and the overall mission of the Law Center through the authorized use of *computing resources* and *data* consistent with the Law Center's need for limited access by persons other than the account holder when necessary to serve or protect operations within the Law Center or to meet legal requirements.

2.0 Policy Scope:

This policy applies to all SULC users. Nothing in this policy is intended or shall be interpreted to waive, limit, or otherwise restrict the rights of the Law Center to manage and allocate use of its *computing resources* and *data* or the responsibilities of *Users* under other SULC policies.

3.0 Policy Compliance:

Failure to with the policy will result in progressive disciplinary action up to and including termination.

4.0 Definitions:

User – SULC employees and students, contractors, vendors, and agents working under the auspices of the Law Center.

Authorized Users - People acting within the scope of a legitimate affiliation with the Law Center, using their approved and assigned credentials and privileges, to gain approved access to Law Center *computing resources*. A person acting outside of a legitimate affiliation with the Law Center or outside the scope of their approved access to Law Center *computing resources* is considered an unauthorized *user*.

Computing Resources - All devices (including, but not limited to, personal computers, laptops, PDAs and smart phones) owned by the Law Center, the *user* or otherwise, which are part of or are used to access (1) the Law Center network, peripherals, and related equipment and software; (2) *data* communications infrastructure, peripherals, and related equipment and software; (3) voice communications infrastructure, peripherals, and related equipment and

software; (4) and all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by the Law Center. *Computing resources* or components thereof may be individually assigned or shared, single-user or multi-user, stand-alone or networked, and/or mobile or stationary.

Content-Neutral Information - Information relating to the operation of systems, including information relating to interactions between individuals and those systems. Such information includes, but is not limited to, operating system logs (e.g., record of actions or events related to the operation of a device or system), *user* login records (e.g., logs of usernames used to connect to Law Center systems, noting source and date/time), dial-up logs (e.g., connections to Law Center modems, noting source, date/time, and caller id), network activity logs (e.g., connections attempted or completed to Law Center systems, with source and date/time), non-content network traffic (e.g., source/destination IP address, port, and protocol), e-mail logs (e.g., logs of e-mail sent or received by individuals using Law Center e-mail systems, noting sender, recipient, and date/time), account/system configuration information, and audit logs (e.g., records of actions taken on Law Center systems, noting date/time).

Data - Include all information that is used by or belongs to the Law Center or that is processed, stored, maintained, transmitted, copied on, or copied from Law Center *computing resources*.

IT Department Member - A person employed, contracted or assigned by Law Center to maintain and operate a computer system or network or any portion thereof. *IT Department Members* are usually charged with installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems.

5.0 Procedure:

General

Except in those circumstances in which access is appropriate to serve or protect operations within the Law Center and to meet legal requirements as outlined in this policy, stored *data*, and voice and *data* network communications will not be accessed by information technology (*IT) Department Member* or anyone other than:

- the person to whom the account in which the *data* has been stored is assigned; or
- the person from whom the communication originated, or to whom the communication was sent; or
- the person to whom the device containing the stored *data* has been assigned.

Although the Law Center seeks to create an atmosphere of privacy with respect to its *data* and use of its *computing resources*, *users* should be aware that because the Law Center is a public institution, and because the Law Center must be able to ensure the security, integrity and continuity of its operations, use of the Law Center's *computing resources* cannot be completely private.

For example, in addition to the types of permissible access described herein, e-mails sent or received through Law Center e-mail accounts, may be subject to disclosure as public records in response to public records requests under Louisiana law. Further, documents including e-mails that are personally identifiable to a student may be education records of that student subject to inspection by that student under federal law. E-mails and other documents and *data* must be accessed by the Law Center to make such determinations. *Users* should be aware that although the Law Center will take reasonable measures to ensure the privacy of Law Center *computing resources as* outlined in this policy, the Law Center cannot guarantee absolute privacy as relates to any particular *User*.

Process

Except as provided herein, an *IT Department Member* at the Law Center may not access or facilitate access to the computer accounts or associated network traffic of someone other than the person to whom the personal computer account or computer is assigned. This includes *data*, voice and other files, including electronic mail (e-mail) and voicemail, encrypted on, stored on, or in transit to or from individual computer or voicemail accounts on Law Center-owned devices/systems, personally-owned devices on Law Center property or devices/systems managed by the Law Center on behalf of affiliated organizations (e.g., Law Center Foundation).

Exceptions

An *IT Department Member* may access or permit access in the following cases:

- Pursuant to authorization from the owner (the individual to whom the account or device or communication has been assigned or attributed);

- To investigate potential violations of law or policy - with written authorization from the Law Center Chancellor's Office for situations where there is reasonable concern that the individual to whom the account or device is assigned or owned has engaged, is engaging, or imminently intends to engage, in illegal activities or violations of Law Center policy using the account or device in question;

- For critical operations - with written authorization from the Department Head of the user's department or Law Center Chancellor's Office for situations in which retrieving the material is critical to the operation of the unit and when the account holder is deceased, terminated, incapacitated, unavailable, or unwilling to provide access;

- On behalf of a deceased or incapacitated individual - with written authorization from Law Center Chancellor's office to provide access to a lawful representative (e.g., spouse, parent, executor, holder of power of attorney) of a deceased or incapacitated employee, faculty member, or student;

- For internal audits - with written request from the Law Center Chancellor's Office or the Southern University System Office Director of Internal Audit for information relating to specific audits or investigations;

- In response to legal process or demand - with written authorization from Law Center Chancellor's Office confirming that access is required under the terms of a valid subpoena, court order, warrant, or other legal demand, or access is required under an applicable law, regulation, or Law Center policy;

- To minimize or mitigate substantial Law Center risk – with written authorization from Law Center Chancellor's Office, Law Center Public Safety Officer, to address an emergency or to avoid or minimize exposure of the Law Center to substantial risk of harm or liability;

- For emergency problem resolution – when the *IT Department Member* has a reasonable concern that a program or process active in the account or on the device is causing or will cause significant system or network degradation, or could cause loss/damage to a system or other *users' data*. This includes forensic and/or other analysis in response to a security incident, sensitive *data* exposure, or system/device compromise;

- To access system-generated, *content-neutral information* – for the purposes of analyzing system and storage utilization, problem troubleshooting, security administration, and in support of audits;

- To investigate security incidents - The incident response function within the SULC IT Department is responsible for investigating reports of abuse or misuse of Law Center *computing resources*. Incident response staff may use system-generated, *content-neutral information* for the purposes of investigating technology misuse incidents, and in support of audits;

- For routine monitoring of network communications - Security personnel in the SULC IT Department may observe, capture, and analyze network communications. Network communications may contain content *data* and in some cases this content may be viewed during analysis. If any *data* must be stored to complete the assigned tasks, it will be stored securely and deleted as soon as possible*;*

- Pursuant to implied consent – in situations where a *user* has requested assistance diagnosing and/or solving a technical problem or where the *IT Department Member* is performing required maintenance. In these cases, the *IT Department Member* shall limit the scope of the access to that which is necessary to address the problem or the task.

- To protect Law Center assets – when there is reasonable concern that the intellectual property, research, trade secrets, or other assets of the Law Center are in jeopardy, and pursuant to written authorization from Law Center Chancellor's Office.

Preservation of electronic information and of *computing resources*

The copying and secure storage of the contents of an individual's e-mail, other computer accounts, office computer, or transient network traffic to prevent destruction and loss of information may occur:

- Upon receiving credible notification of a Law Center or law enforcement investigation for alleged illegal activity or violations of Law Center policy on the part of a member of the Law Center community;

- Upon receiving advice by the Law Center's legal counsel that such copying and storage is otherwise needed in order to comply with legal obligations to preserve electronic information or secure *computing resources*;

- Upon receiving authorization from the Law Center Chancellor's Office, or Law Center Safety Officer, or the Southern University Police Department official indicating that such preservation reasonably appears necessary to protect Law Center operations;

- When there is a reasonable concern that illegal activity or violations of Law Center policy have occurred, are occurring, or are imminent, as determined by the SULC IT Department;

- As a routine backup procedure for disaster recovery or archival purposes. *Note:* Access to such copies and stored materials shall be in accordance with this policy. Preserved materials that are no longer needed shall be destroyed in a secure manner.

General Duties of *IT Department Members* Accessing Computing Resources

Maintain the privacy of both the contents and the act of the access, except as otherwise required by this policy, or when necessary to report potential violations of law or Law Center policy, and then only to the appropriate authority;

Make reasonable efforts to report such actions to the affected individual prior to that access, except when:

- Prior notification is not appropriate or practical due to the urgency of the circumstances;

- Such notice may result in destruction, removal, or alteration of data;

- Other circumstances make prior notice inappropriate or impractical.

Where prior notification is not appropriate or practical, reasonable efforts will be made to notify the affected individual as soon as reasonable under the circumstances. No notification is necessary if access is for strictly routine backup, disaster recovery, or for archival purposes.

Coordination with SULC IT Department:

All requests for access to computer accounts must be coordinated with the SULC IT Department. Where needed, proper and authorization must be presented to the IT Department before access is accorded.

Legal Requests or Demands

All legal requests or demands for access to *computing resources* or electronic information and all subpoenas, warrants, court orders, and other legal process, or demands directing that access be afforded to law enforcement agencies or others, must be delivered immediately to the Law Center Chancellor's for verification and approval. Should such documents be served on individual, employees, or *IT Department Member*, the documents must be sent immediately to the Law Center Chancellor's office for review.

The Law Center Chancellor's office for review will review the request or order, and advise the relevant personnel on the necessary response. In the event that a law enforcement agency seeks to execute a search warrant or other order immediately and will not wait for review, individual *IT Department Member* or other persons receiving such orders should not obstruct the execution of the warrant or order, but should document the actions by law enforcement, notify the Law Center Chancellor's office for review as soon as possible, and take reasonable steps whenever possible to preserve a copy of any *data* being removed, for appropriate Law Center use.

Initiating Access

Persons seeking access to specific *computing resources* and/or electronic information assigned to or associated with an individual, that are maintained by the SULC IT Department must send those requests to the Law Center Chancellor's Office. In addition, persons seeking access to specific *computing resources* and electronic information primarily assigned or associated with other persons, and that are not maintained by SULC IT Department (e.g. computing resources maintained by the Southern University) should direct those requests to the Law Center Chancellor's office for approval, disposition, or forwarding to appropriate officials.

APPROVED: Lata Johnson **DATE:** 7/15/2019