□

□

□

□

□

□

□

□

□

□

# Non-Consensual Access to Electronic Information Resources

**Request Form**

Use this form to request non-consensual access to electronic files or communications as provided under SPC policy (IA-Policy Compliance).

|  |
| --- |
| A. REQUESTOR NAME, TITLE AND DEPARTMENT |
| **Full Name, Title and Department of requestor:** |

|  |
| --- |
| B. ANNUAL AUTHORIZATION (Must comply with SHSU Policy IT-00) |
| The following staff members have blanket approval to access data on the SPC network to fulfill his/her duties for FY \_/ \_. |

|  |
| --- |
| C. ONE-TIME ACCESS BASIS FOR REQUEST (Must comply with SPC Policy IA-Policy Compliance) |
| **Provisions under which records are to be accessed**(check all that apply):Required by and consistent with law or policy Legal obligation (subpoena, court order, etc.)Protect and sustain the operational performance and integrity of university information systems and business processes.Review, audit, or investigations by authorized partyProtect legitimate interests of university or other users. | **Reason(s) why holder’s consent cannot be obtained**(check all that apply):Holder has denied a request to allow accessAbsence, illness or death precludes requesting holder’s consent Compelling circumstances preclude requesting the holder’s consent (describe in comment) Post-authorization: the records have already been accessed to address time-dependent, critical operational needs Record holder is no longer an employee or student |
| **Comments: (**Record holders Network ID, account name(s), system name(s), or folder name(s)) |

|  |
| --- |
| D. REQUESTING PARTY/DEPARTMENT HEAD SIGNATURES |
| **Signature of Requesting Party: Date Signature of Department Head: \_Date \_ Printed Name of Department Head:**  |

|  |
| --- |
| E. APPROVAL OF IRM OR DESIGNEE (Required for All) |
| **Non-Consensual access authorized? Yes No****Signature of IRM or Designee: \_Date \_ Printed Name \_** |

# Non-Consensual Access to Electronic Information Resources

**Request Form Procedures**

Policy Background:

SPC places a high value on individual privacy and recognizes its importance in an academic setting. The College generally prohibits access to stored electronic records and voice and data communications by other than the designated owner of the computer account or electronic resource containing the information or communication, or, the sender or recipient of a particular communication, unless prior consent has been granted by the applicable owner, sender, or recipient.

SPC cannot absolutely guarantee the privacy or confidentiality of electronic documents. Consistent with Texas Administrative Code Chapter 202, Rule 202.75(9), users should not expect privacy in their use of Texas State information technology resources. Consequently persons that use these SPC-owned resources, or any personally owned device that may be connected to an SPC resource, have no right to privacy in their use of these resources and devices.

However, SPC will take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons that SPC will not seek access to their electronic messages or documents without their prior consent except where necessary to:

* Satisfy the requirements of the Texas Public Information Act, or other statutes, laws or regulations;
* Satisfy other legal obligations, such as subpoenas and court orders;
* Protect and sustain the operational performance and integrity of university information systems and business processes;
* Facilitate security reviews, audits, and investigations by authorized individuals in the performance of their assigned duties;
* Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergency situations;
* Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;
* Protect and support the legitimate interests of the university and other users, as determined by the IRM and ISO.

Procedures for Obtaining Non-Consensual Access to Electronic Records:

To appropriately preserve the privacy of electronic documents and allow authorized individuals to perform their assigned duties, specific university staff and law enforcement will sign an

SPC Non-Consensual Access to Electronic Information Resources Request Form annually and submit the form to the Office of the Information Resources Manager (IRM). At the beginning of each fiscal year, non-consensual access requests will be resubmitted, reviewed, and approved or denied by the IRM.

Individuals may request non-consensual access to specific data by initiating the attached Non- Consensual Access to Electronic Information Resources Request Form, obtaining the approval of their organizational head, and submitting the form to the Office of the Information Resources Manager (IRM). If the request appears compliant with university policy, the IRM or designee will coordinate with the Information Security Officer (ISO) as necessary to satisfy the request. Perusal will be limited only to the records that satisfy the criteria specified in the request.