SSRI IT Policies

Updated: January, 2018 (reviewed annually)

Scope

These policies apply to staff, faculty, and affiliates of SSRI, including servers, network equipment and storage devices.

Compliance

All SSRI staff, faculty, and affiliates must comply with SSRI IT policies (posted on the SSRI website), and with all applicable state and federal laws and regulations. Faculty, staff, and affiliates have a responsibility to use SSRI IT resources in an efficient, effective, ethical, and lawful manner. Violations of the policy may result in loss of usage privileges, administrative sanctions (including termination or expulsion) as outlined in applicable Duke University disciplinary procedures, as well as personal civil and/or criminal liability.

These policies are subject to review and audit by Duke's Office of Internal Audit.

Responsibility

SSRI is responsible for implementing the policies described in this document.

Authority

SSRI IT operates under authority of the Associate Director of IT and the Director of SSRI.

SSRI Policies that affect PRDN operations & administration

SSRI Workstation and Laptop policy

SSRI staff who access Sensitive data (https://security.duke.edu/policies-standards-procedures) as part of their job duties will only do so from SSRI-managed machines that comply with the ITSO technical standards for workstations and laptops. (See link above.)

SSRI Security or Privacy Incident policy

A security incident is:

- an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information
- interference with the operation of an information system

If a security incident is suspected or confirmed, SSRI staff will gather as much of this information as possible:

- All user IDs and systems involved in the incident.
- Identify all business processes or applications affected.
- Does the system or application involved store or process Sensitive or Restricted data?

- Does the user involved have access to Sensitive or Restricted Duke data as a part of their job duties?

SSRI faculty, staff, and end users will report suspected security incidents to SSRI IT staff (ssricomputing@duke.edu). If an incident involving SSRI systems, users, or Sensitive data appears to be more than a simple malware infection, or involves exposure of multiple systems, accounts, or exposure of Sensitive data, SSRI staff will follow the University policy and report the incident to the University IT Security Office (security@duke.edu).

If a request is received (whether from internal or external requestors) for information that would identify a Duke user or provide access to a Duke user's data, SSRI will report that request to the University IT Security Office and will not act on it without prior authorization by ITSO.

Most of SSRI is engaged in activities that require faculty, staff, researchers and students to have access to protected data – data classified as Sensitive or Restricted according to the Duke Data Classification standard. These are categories of data that Duke is either required by law to protect, or which Duke protects to mitigate institutional risk. In these cases, personnel who access protected data must abide by strict safeguards regarding access to data, e-mail, departmental computers, personal laptops and other electronic devices.

For this reason, the following requirements apply to SSRI staff, faculty, and affiliates:

- **Computers**: To prevent unauthorized access to information and resources, Duke-owned computers must be configured with appropriate technical controls. Duke owned computers accessing Sensitive data must be managed by SSRI's IT team to ensure that the devices are configured to comply with the University IT Security Office's technical standards.
- **Computers**: Personal phones, laptops, desktops, and other devices should not be used to access Sensitive or Restricted Duke data.
- **Email**: All Duke related communication, regardless of whether it contains protected information or not, must be conducted within the Duke managed email system. SSRI IT support staff can help configure or make recommendations for configuring mail clients to access Duke email services.
- **Portable Data storage**: If protected storage environments are not easily accessible for activity related to working with protected Duke data, then use of portable storage devices can be supported. Any portable storage devices (thumb drives, external hard drives) should be encrypted using methods identified by the Duke IT Security Office or SSRI IT support staff.