NIU Data Center Access Policy

Purpose

NIU data center facilities are secured areas. Entry is prohibited except for authorized individuals, and those they accompany, for official university purposes only. This policy governs access to the NIU data center locations.

Policy

Authorization

University employees that need access to a NIU data center location, must complete the Facilities Key Control and Division of IT (DoIT) authorization and approval process. Those that have been authorized will receive OneCard swipe access to only the data center location needed. In addition, some employees in Facilities and the Division of IT will have approval for physical key access based on required job duties.

If the University enters a contract with a vendor for paid support services that requires frequent access to a NIU data center location, the vendor must provide proof of their staff’s background check or NIU must perform a background check; the Department owning the contract must follow the sponsored account process for the vendor’s staff member; and each vendor staff member must be explicitly approved by the authorization process above before being issued an individual OneCard for swipe card access to the data center facilities. The sponsoring Department is responsible for the cost of the sponsored account OneCard. The sponsoring Department is responsible for requesting revocation of sponsored account access as soon as they are aware that the sponsored individual no longer needs access.

Any individual not explicitly approved by the authorization process above, hereby designated as a third party, may not access a NIU data center unless:

1. Prior approval by the Office of Information Security has been granted
2. They are escorted at all times by someone that has been authorized for access

Access

All authorized employees must use card swipe for access unless key access is required. Tail-gating or “piggy backing” on someone else’s swipe card is not allowed. Each authorized person should swipe for their own access. All staff who enter without swiping, regardless of whether they have a card access or not, must sign in.

Every third party must sign in and sign out on the access log located near the door of each facility. It is the responsibility of the employee escort to ensure that the third party signs this logbook. The escort is also responsible to ensure that third party access be restricted to the immediate area surrounding the systems that the escort and/or third party is authorized to access.
Everyone that signs the log must state the reason for their visit. Examples could be: XYZ server maintenance, SMRF #1234, work order #1234, project #1234, etc. Access is limited only to those areas, racks, and systems the employee is authorized for.

Hours of access for authorized individuals that are not Division of IT or Facilities staff, are Monday-Friday 7:00am-5:00pm. Authorized individuals requesting access to a DoIT facility after hours, are required to follow the Division of IT after hours on call support model and will be charged $35/hr with a minimum of two hours charged.

Access for non-DoIT, and non-Facilities employees expires annually and must be renewed.

Access will be revoked immediately upon separation from the University.

**Tours**

Tours may be scheduled with the Division of IT at least one month in advance. A list of individuals participating in the tour should be supplied by the person requesting the tour. The list should be attached to the sign-in log and the individual requesting the tour must sign in for the tour group. Recording devices are prohibited. Exceptions made by the Office of Information Security only.

A member of DoIT staff or management will escort the authorized individuals into the facility.

**Conduct**

The following rules of conduct apply to all who enter the computer and network facilities:

- They shall not allow unauthorized or unapproved personnel into the NIU computer and network facilities without following this policy.
- They shall not access, handle, or tamper with ANY equipment they are not explicitly authorized to access. This includes, but is not limited to, access controls, HVAC, power, fire suppression, floor tiles, cables, racks, cameras, servers, network equipment, tools, etc.
- They shall not bring wet clothing and belongings such as umbrellas, coats, bags, etc. into the computer and networking facilities.
- They shall not bring food or drink into the facilities.
- They shall place all small amounts of trash in containers provided or take it with them when they leave. Large volumes of trash such as cardboard boxes and shipping materials must be removed from the facility and disposed of off-site.
- They shall keep areas of approved access clean and clear of debris at all times. Spare parts, supplies, tools etc., are to be kept in a previously arranged or contracted storage location.
- They are prohibited from taking pictures or videos, or any other recording, in the facility unless previously approved by the Office of Information Security.
- They shall not prop open unattended doors in the facilities.
- They shall ensure facility doors are closed and secure when they leave.

**Incident Reporting**

All events that have any potential negative consequences for the management of the data center, the equipment therein, or the confidentiality, integrity and availability of the data and network, must be
reported to the Division of Information Technology Service Desk as soon as possible after discovery. DoIT will review the event to determine what response is necessary.

Examples of events may be:

- Data center door found unlocked.
- Evidence of un-authorized physical access to a rack, system, cables, floor tiles or equipment.
- Evidence of water, fire, excessive room temperature, excessive rack or system temperature, electrical problem, or any other hazard.
- Evidence of unauthorized data recording, storage or tampering devices.

**Compliance**

Anyone who is found not in compliance with this policy will have their authorization to access the NIU computer and network facilities revoked, and university corrective action will be administered up to and including termination depending on the severity of the situation.