LONG ISLAND UNIVERSITY

THIRD-PARTY ACCESS POLICY

PURPOSE

The purpose of this policy is to define standards for connecting to LIU Information Technology resources. These standards are designed to minimize the potential exposure to LIU from damages which may result from unauthorized use of LIU information technology resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical LIU internal systems, etc.

STATEMENT OF POLICY

As a condition of gaining access to LIU information technology resources, the following requirements must be met for any third-party organization conducting official business with Long Island University by accessing IT infrastructure.

Compliance Requirements:

1. Every third-party must sign an LIU Non-Disclosure Agreement.
2. All third parties must be sponsored by an authorized LIU Officer.
3. All third parties must adhere to FERPA, GLBA, HIPAA, NY State Privacy Act, and other applicable privacy and security regulations (federal and New York state).
4. Adherence to LIU's single sign-on methodology with Duo two-factor authentication.
5. All third-party agreements and contracts must specify:
    a. The LIU information to which the third party has access.
    b. How LIU's information is to be protected by the third-party.
    c. Acceptable methods for the return, destruction, or disposal of LIU's information in the third-party's possession at the end of the contract.
6. Third-party personnel must report all security incidents immediately to the appropriate LIU sponsor and the Information Security Team.
7. Any third-party account holder that violates this policy will have the account suspended and the account holder's sponsor will be notified. Following a review, LIU will implement the actions specified by LIU Information Security polices to reinstate or remove the account and escalate to appropriate officials and authorities, as deemed necessary.

Information System Infrastructure Requirements:

1. Proof of third-party penetration test or security assessment within that last year. This must include all critical organization assets.
2. Proof of certification of applicable standards, for example, PCI-DSS, HIPAA, SOC2.
3. Provide a document outlining the security baselines used for each server and workstation build.

4. Provide a backup plan, including retention times and whether backups are stored offline, are encrypted, and are isolated from the primary identity infrastructure.
5. Provide security patch deployment plan, which includes plan for apply critical (0-day) patches, as well as monthly security patches.
6. Provide current Disaster Recovery Plan and Business Continuity Plan for critical IT infrastructure.
7. Provide documentation on server and workstation EDR/XDR deployments that are used on critical IT assets.
8. Provide network firewall and IDS/IPS deployment strategy for critical IT infrastructure. Provide basic network diagram with obfuscated sensitive information if possible.
9. Provide application flow diagram of systems that will integrate with LIU IT systems.
10. Provide evidence of security awareness training policy and whether phishing simulations are run.
11. This Third-Party Access Policy pertains to all third-party organizations and individuals that require access to non-public electronic resources maintained by Long Island University.

POLICY TYPE: OPERATIONS

LAST REVIEWED: JANUARY 2023