Third-Party Access to University IT Resources Standard

Background

Third-party vendors play an important role in the support of hardware and software management and operations. Third parties may have the ability to remotely view, copy or modify data, correct software and operating system problems, monitor systems and fine tune system performance. Setting limits and implementing controls must be done to reduce risk to the university.

This standard is applicable to all third-party users (also called “affiliates”) connecting to the university’s network, either internally or via remote access.

Standard

The vendor contract must contain contractual language making adherence to this standard mandatory and the contract must include the Data Security Rider. The university department contracting with the third party is responsible and must insure the third party is compliant with the following standards:

1. Affiliates must access the universities network using the provided account.
2. Affiliates must use the university provided VPN and must use university approved multi-factor authentication when accessing university IT resources.
3. Servers located in a university owned data center must be separated on an isolated network within the data center and follow the best practices of Network Isolation and Segmentation.
4. Affiliates must utilize access that is consistent with the principle of Least Privilege.
5. Affiliates must comply with all university Policy, Procedures, Standards and Guidelines.
6. Affiliates must comply with all federal and state laws and regulations including but not limited to FERPA, HIPAA, PCI-DSS and FISMA.
7. Affiliates must complete a Non-Disclosure Agreement (NDA) prior to accessing Controlled or Restricted university data and affiliate sponsor must maintain all NDA records.
8. Affiliates must use university data and IT resources only for the purpose as stated in the business agreement or contract.
9. Affiliates must immediately report all information security incidents to the IT@UC Office of Information Security, abuse@uc.edu.
10. Affiliates must follow all applicable university change control processes and procedures.
11. Affiliates must use software that is properly licensed and appropriately up to date.

12. Affiliates must adhere to the Data Center Visitor Policy when accessing any university data center.
13. Affiliates must adhere to the applicable safeguards in the Data Governance & Classification Policy.
14. Affiliates must maintain user access and login information. Security logs must be maintained and forwarded to the IT@UC Office of Information Security centralized logging solution.
15. Affiliates must provide UC with a list of all personnel working on the contract. The list must be updated and provided to UC within 48 hours of changes in personnel assignments.
16. Affiliates must have a background check if working, accessing or have access to university restricted data as classified in the Data Governance & Classification Policy.
17. Affiliates must be a citizen or a permanent resident ("green card") of the United States of America. Non-immigrant foreign nationals are not permitted to have access to servers located in a university data center.

Related Links

Data Governance & Classification Policy
Data Center Visitor Policy
Non-Disclosure Agreement

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) Email: infosec@uc.edu

History

Created: 2/28/2017