University of New Haven

Policies and Procedures

Policy Title: Office of Information Technology Third Party Access

Policy No.: 7015 Rev.: 0
Effective Date: November 12, 2014
Last Revision: November 12, 2014

Responsible Office: Office of Information Technology
Responsible Official: Associate Vice President for Technology & CIO

Contents

Scope

The University of New Haven Third-Party Access Policy outlines responsibilities and expectations of any individual from an outside source (contracted or otherwise) who requires access to our information systems for the purpose of performing work. This policy also outlines the responsibilities and expectations of The University of New Haven personnel responsible for the contracting and/or supervising of the third party.

Policy Statement

University owned information technology resources and equipment must be kept in a secure area to minimize the threat of damage caused by intentional or unintentional actions. Only authorized members of the Office of Information Technology can gain access to these secure areas. University network systems are also kept secure to minimize the threat of malicious attacks on our information systems. Only members of the university community, including students, faculty and staff, have access to the university network.

Reason for the Policy

The Purpose of The University of New Haven's Third-Party Access Policy is to establish the rules for third-party access to The University of New Haven information systems and the computer room, third-party responsibilities, and protection of The University of New Haven information.

Definitions

Third Party
A third party could consist of, but is not limited to: software vendors, contractors, consultants, business partners, and security companies.

Computer Room
Secure area where university computer and network equipment are located.

OIT
Office of Information Technology

Policy Sections

7015.1 Computer Room Third Party Policy Guidelines.

1. All third-party access to the computer center should be scheduled to occur during regular business hours. If this is not possible, a point person from the OIT

department will be scheduled after hours to accompany the third party.
2. When third parties are scheduled to have access to the computer center, the OIT staff must be notified in advance of the date, time, and type of work to be performed.
3. When the third party arrives, he/she will report to a staff contact that scheduled the visit. The staff contact will escort the third party to the OIT area. At this point, the third party is to be informed that he/she will take further direction from the OIT staff point person in relation to their activity in the computer center.
4. Prior to the onset of any work, the third party will describe the activities that are planned.
5. The OIT staff point person is responsible for explaining what measures need to be taken to protect the computer hardware and software, explain protective measures to the third party, and ensure that the measures come to fruition. In an attempt to offset delays in the work of the third-party individual(s), the OIT staff will attempt to minimize the delays within the constraint of safeguarding the systems. The third party will need to clearly understand that they are to allow time for the OIT staff to do what needs to be done to protect the computer systems before starting their work.
6. The third party will report to and receive instructions from the OIT staff point person regarding their work in the computer center. The OIT staff point person will also be kept informed of the status of the work, as well as the notification that the work is completed before leaving the area.

7015.2 Information Systems Third Party Policy Guidelines

1. Any third-party agreements and contracts must specify:

    - The work that is to be accomplished and work hours. Also, any configuration information of any installed software as well as virus checking of that software.
    - The University of New Haven information that the third party should have access to.
    - The minimum security requirements that the third party must meet (i.e., method for remote access).
    - How the University of New Haven information is to be guarded by the third party. Signing of a non-disclosure agreement is typically required.
    - Strict use of the University of New Haven's information and information resources for the purpose of the business agreement by the third party. Any other information acquired by the third party in the course of the contract cannot be used for the third-party's own purposes or divulged to others.
    - Feasible methods for the destruction, disposal, or return of the University of New Haven information at the end of the contract.

- The return of company property such as a laptop, PDA, or cell phone after the completion or termination of the agreement.

2. The third party must comply with all applicable university standards, agreements, practices and policies, including, but not limited to:

   - Acceptable use policies.
   - Software licensing policies.
   - Safety policies.
   - Auditing policies.
   - Security policies.
   - Non-disclosure policies.
   - Privacy policies.

3. The University of New Haven will provide an OIT point of contact for the third party whether it is one person from the OIT department or an interdepartmental team. This point of contact will liaise with the third party to ensure they are in compliance with these policies.

4. The third party will provide the University of New Haven with a list of all additional third parties working on the contract. The list must be updated and provided to the University of New Haven within 48 hrs of any staff changes.

5. Third party access to systems must be uniquely identifiable and authenticated, and password management must comply with the University of New Haven's Password Policy. Managing connectivity with partner networks can be handled different ways depending on what technologies are in place (i.e. encryption, intrusion detection, DMZ architecture).

6. Any third party computer/laptop/PDA/tablet PC that is connected to the University of New Haven systems must have up-to-date virus protection and patches. The third party will be held accountable for any damage occurred to the University of New Haven in the event that an incident occurs.

7. Each third-party employee that has access to the University of New Haven's sensitive information should be cleared by the CIO to handle that information.

8. If applicable, an explanation of how the University of New Haven information will be handled and protected at the third party's facility/site must be addressed.

9. Third-party employees must report all security incidences to the appropriate university personnel.

10. If third-party management is involved in the University of New Haven's security incident management, the responsibilities and details must be specified in the contract.

11. The third party must follow all applicable change control procedures and processes.

12. All software used by the third party in providing service to the University of New Haven must be properly inventoried and licensed.

13. All third-party employees are required to comply with all applicable auditing regulations and the University of New Haven auditing requirements, including the auditing of the third-party's work.

14. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate university management.

15. All third-party maintenance equipment on the university's network that connects to the outside world via telephone lines, leased line, or the network will remain disabled except when in use for authorized maintenance.

16. The third party's major accomplishments must be documented and available to the University of New Haven's management upon request. Documentation should include, but is not limited to events such as:

    - Personnel changes.
    - Password changes.
    - Project milestones.
    - Deliverables.
    - Arrival and departure times.

17. Upon departure of the third party from the contract for any reason, the third party will ensure that all sensitive information is collected and returned to the university or destroyed immediately upon departure. The third party will also provide written certification of that destruction within 24 hrs. All equipment and supplies must also be returned, as well as any access cards and identification badges. All equipment and supplies retained by the third party must be documented by authorized University of New Haven management.

18. The University of New Haven will perform an impact analysis of other business-critical functions, once work has begun by the third party.

19. The University of New Haven will monitor system and network log files 3 times per week.

20. The University of New Haven will eliminate third-party access to facilities after the contract has been completed or terminated. The following steps must be performed:

    - Remove third party authentication and all means of access to systems.
    - If needed, make sure that incoming e-mail is re-routed to an appropriate person.
    - Archive any third-party software configuration, and transfer ownership to designated internal staff.
    - Get a written statement from the third party that any software created and/or installed by the third-party is free of viruses and any other malicious code.

7015.3 Enforcement

Any employee or third party who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.