FAIRLEIGH DICKINSON UNIVERSITY

Vendor Access Policy
for Networking & Computing

Author	Date	Version	Description
Stuart Alper,	2/7/2023	1.0	**First Revision**
Christopher Robley			
	2/8/2023	1.1	**Second Revision**
Neal Sturm	2/14/2023	1.2	**Changes on requiring Laptop language**

This policy is managed by the Director of Systems within the University Systems & Networking department.

Table of Contents

Effective Date: 3/01/2023
Last Revision: 03/1/2023
Last Review:

Introduction

As the demand for access by on-site vendors increases, Fairleigh Dickinson University has created a Vendor Access Policy for Networking and Computing. The intent of the policy is to define the categories of non-employees that are on our campuses and provide rules and guidelines around their networking & computing needs. All business units should utilize the Contract Review Process which has been instituted by the Office of the General Counsel prior to initiating any of the below processes. Fully executed contracts that have been reviewed and approved may be requested by members of OIRT prior to providing any access for the non-employees below.

Contractors/Consultants

The University employs individuals from companies that perform work on behalf of the University and expressly for the University. Examples could be an employee from a staffing agency working within IT to augment the staff in assisting with a series of projects, or an individual hired from an agency to work within Human Resources to assist in processing forms. These individuals are hired under contracts and are held to the terms and conditions of those contracts. In most cases, working as part of the University, these individuals need computing functionality identical to those of university hired staff, as they are acting on behalf of the University & fulfilling a role specific to the University. All work done by these individuals is part of the universities data property, and therefore, careful consideration needs to be given to providing these individuals with University issued devices such as desktop/laptop computers, landline phone extensions, etc.

Individuals hired from companies outside of the University to conduct business on behalf of the University must meet the following guidelines and are provided with the following access:

1. Contractors/Consultants will be issued a University NetID & email address in the standard Firstinitial.Lastname@fdu.edu format.
2. All Contractors/Consultants are required to complete the Written Information Security Program (WISP) training immediately after an account is provisioned. Validation of completion is needed within first 30 days.
    a. WISP training reminder at day 15
    b. WISP training daily reminder every day after day 15
    c. Disable account day 30 with an email sent to the manager.
3. All contractors/consultants must read and accept the following additional policies:
    a. Policy for the acceptable use of email
    b. Acceptable use policy for computer usage
    c. FDU alert policy
    d. Password policy
4. Contractors/Consultants will be able to sign up for FDU Alert through Colleague Self-service. Instructions can be found at https://it.fdu.edu/self-service-tutorial/
5. Contractors/consultants deemed necessary to be issued University managed laptops/desktops will be at the expense the hiring department.
6. Upon departmental request, contractors/consultants will be provided access to specific university systems and applications based on overall business needs. These requests will be reviewed by the Director of Systems.
7. All contractor/consultant accounts will expire at the end of the fiscal year (June 30th) and must be renewed by the FDU manager by completing a Personal Information Notice (PIN) form.
8. Contractors/consultants must be terminated at the end of their contract using the same methodology utilized for current faculty and staff. It is the unshared responsibility of the managing department to submit termination paperwork per the HR process for any contractor/consultant who had been issued a NetID.

Volunteers

The University utilizes volunteers in non-paying positions during the school year. Examples of these roles include but are not limited to preceptors & chaplains. These individuals do not need access to any University systems with the exception of email. As such, they need access to Internet services & email but they do not require an FDU managed laptop/desktop.

Volunteers must meet the following guidelines and are provided the following access:

1. Volunteers will be issued a NetID in the format of Firstinitial.Lastname@v.fdu.edu to be able to authenticate to FDU's wireless network (and wired network in the future).
2. Volunteers are required to complete the Written Information Security Program (WISP) training immediately after an account is provisioned. Validation of completion is needed within first 30 days.
    a. WISP training reminder at day 15
    b. WISP training daily reminder every day after day 15
    c. Disable account day 30 with an email sent to the manager.
3. All volunteers must read and except the following additional policies:
    a. Policy for the acceptable use of email
    b. Acceptable use policy for computer usage
    c. FDU alert policy
    d. Password policy
4. Volunteers will be able to sign up for FDU Alert through Colleague Self-service. Instructions can be found at https://it.fdu.edu/self-service-tutorial/
5. All volunteer accounts will expire at the end of the fiscal year and must be renewed by their FDU manager by completing a PIN form.
6. Volunteers must be terminated at the end of their contract using the same methodology utilized for current faculty and staff. It is the unshared responsibility of the managing department to submit termination paperwork per the HR process for any contractor/consultant who had been issued a NetID.

On-Campus Vendors

The University outsources various functions to entities (Vendors) that operate independently but work exclusively on our campuses and provide services for our faculty, staff & students. These employees are individually managed by their corporate entities and are largely held accountable by their corporate management.

While on campus, employees of these vendors might need access to the Internet to interact with their corporate websites or communicate to their corporate managers. In many cases today and in most all cases in the future, these employees will need to authenticate through the University's network in order to conduct their business. The University has established a process whereby the Fairleigh Dickinson University department responsible for that vendor completes the Human Resource forms necessary in order to create a non-employee record within our Colleague system.

Employees of on-campus vendors must meet the following guidelines and are provided the following access:

1. Vendor employees will be issued a NetID in the format of Firstinitial.Lastname@v.fdu.edu to be able to authenticate to FDU's wireless network (and wired network in the future).
3. Vendor employees will be able to add their contact information to FDU Alert by sending an email to fdunotify@fdu.edu
4. All vendor employee accounts will expire at the end of the fiscal year and must be renewed by their FDU manager by completing a PIN form.
5. Vendor employees must be terminated through FDU's systems when they either are removed from their assignment at Fairleigh Dickinson University or are terminated by their employer using the same methodology utilized for current faculty and staff. It is the unshared responsibility of the managing department to submit termination paperwork per the HR process for any contractor/consultant who had been issued a NetID.

Elevated Vendor Privileges

From time to time, the employee of an on-campus vendor might have justification for having access to FDU email or a need to access systems and/or applications that reside behind FDU's firewalls. If such a case is identified, the FDU department responsible for that vendor would need to contact the Director of Systems with a formal request for additional vendor access. The FDU department must present solid business justification for the elevated access. The Director of Systems will review each request and either approve or reject the request based on business need and security posture. The Director of Systems might consult with the Data Security & Incident Response Team before providing an answer.

Employees of on-campus vendors approved for elevated access must meet the following guidelines and are provided the following access:

1. Vendor employees will be issued a NetID in the format of Firstinitial.Lastname@v.fdu.edu to be able to access FDU's wireless network (and wired network in the future).
2. All vendor employees are required to complete the Written Information Security Program (WISP) training immediately after an account is provisioned. Validation of completion is needed within first 30 days.
    a. WISP training reminder at day 15
    b. WISP training daily reminder every day after day 15
    c. Disable account day 30 with an email sent to the manager.
3. Vendor employees will be able to sign up for FDU Alert through self-service. Instructions can be found at https://it.fdu.edu/self-service-tutorial/
4. All vendor employees with elevated access must read the following additional policies:
    a. Policy for the acceptable use of email
    b. Acceptable use policy for computer usage
    c. FDU alert policy
    d. Password policy
5. If the vendor employee needs to access FDU systems and/or applications, issuance of a University managed laptop/desktop may be required. This would be at the expense of the requesting department.
6. Upon departmental request, vendor employees will only be provided access to the specific University Systems and applications approved by the Director of Systems.

7. All vendor employee accounts will expire at the end of the fiscal year and must be renewed by their FDU manager by completing a PIN form.
8. Vendor employees must be terminated through FDU's systems when they either are removed from their assignment at Fairleigh Dickinson University or are terminated by their employer using the same methodology utilized for current faculty and staff. It is the unshared responsibility of the managing department to submit termination paperwork per the HR process for any contractor/consultant who had been issued a NetID.