Elmhurst College

# Network and System Access and Security Policy

## 1. Overview

Access to Elmhurst College's networks and systems is essential to support many educational activities and operational functions. Standards for on-campus network and system access are designed to allow appropriate use of networks and systems by the many individuals and groups the College legitimately serves while doing as much as possible to manage the risks to both individuals and College systems posed by the use of modern networks. Remote access to the Elmhurst College's networks and systems can also be essential at times, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our Elmhurst College network. While these remote networks are beyond the control of Elmhurst College policy, we must mitigate these external risks to the best of our ability.

## 2. Purpose

The purpose of this policy is to define rules and requirements for connecting to Elmhurst College's networks and systems from any host. These rules and requirements are designed to minimize the potential exposure to students, employees, contractors, vendors, guests, and other affiliates of Elmhurst College as well to the College itself from damages which may result from unauthorized use of Elmhurst College resources. Potential damages include but are not limited to the loss of sensitive or confidential data or intellectual property, damage to public image, damage to critical Elmhurst College internal systems, and fines or other financial liabilities that could be incurred as a result of those losses.

## 3. Scope

This policy applies to all Elmhurst College students, employees, contractors, vendors, guests, and others who connect to Elmhurst College's networks and systems using any computing device, whether owned by Elmhurst College or not. This policy applies to both on-campus network connections and remote access connections used to interact on behalf of Elmhurst College. This policy covers any and all technical implementations of local or remote access used to connect to Elmhurst College networks.

## 4. Policy

It is the responsibility of Elmhurst College students, employees, contractors, vendors, guests and others with access privileges to Elmhurst College's networks and systems to ensure that their access connections, whether on campus or remote, meet all necessary security requirements and conform to all College policies. Access to the Elmhurst College network is strictly limited to authorized users as articulated by the Office of Information Services (OIS). Access privileges to Elmhurst College's networks and systems may be declined, suspended, or revoked at any time for violations to policies or operating procedures or if necessary to accommodate network maintenance or other changes. Authorized users accessing Elmhurst College's networks and systems from a personal or other non-College owned computing device are responsible for preventing access to any Elmhurst College computer resources or data by non-authorized users. Performance of illegal activities through the Elmhurst College network by any user, authorized or otherwise, is prohibited. Authorized users will not use Elmhurst College networks to access the Internet for outside business interests.

All authorized users bear responsibility for and the consequences of misuse of network and system access privileges. For further information and definitions, see the *Acceptable Use Policy*. For additional information regarding Elmhurst College's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., contact the Elmhurst College Help Desk.

4.1 Network and System Access

4.1.1 Access to Elmhurst College's network is generally made available through an Elmhurst College Technology Account provided by the Office of Information Services (OIS). Technology Account credentials are personal and may not be shared with anyone at any time. Levels of network access are based on educational and job requirements and are managed by OIS. Limited temporary or guest access to the Elmhurst College network may be available based on need and will be issued by OIS in accordance with appropriate administrative approval.

4.1.2 Technology account credentials must conform to the *Password Policy* and any other security requirements articulated by OIS.

4.1.3 All system accounts will be issued and managed by OIS in accordance with its procedures for identity and access management.

4.1.4 Access to Elmhurst College's networks and systems is a privilege which may be revoked for violation of federal, state, or local law, violation of College policy, or engagement in any prohibited network use or action.

4.2 Prohibited Uses and Actions

4.2.1 Use for purposes that violate federal, state, or local laws, including copyright laws that prohibit the downloading or distribution of copyright protected data such as music, video, videogames, etc.

4.2.2 Use for a private enterprise or not-for-profit organization unless authorized by the College.

4.2.3 Use in any way that interferes with or disrupts other network users, services, or equipment.

4.2.4 Accessing sites that are pornographic or offensive in nature.

4.2.5 Accessing or attempting to access restricted data files, software or systems without authorization.

4.2.6 Creating or transmitting lewd, obscene, hateful, bigoted, or discriminatory material or information.

4.2.7 Concealing or misrepresenting one's name or affiliation to mask irresponsible or offensive electronic communication.

4.2.8 Using electronic mail or other network communications to harass, offend, or annoy other users.

4.2.9 Sending chain letters through electronic mail.

4.2.10 Actions which violate any other College policy.

4.3 Remote access

The Elmhurst College Virtual Office provides secure VPN access to on-campus resources from offsite via RDP, Tunnel, VNC, and iOS or Android devices. The VPN also allows authorized users to create a secure connection between their remote computer and the private campus network, allowing access to systems and devices including Colleague, Informer, and network storage devices. Policies and procedures for obtaining and using VPN access are as follows:

4.3.1 Use of external resources to conduct Elmhurst College business must be approved in advance by the Office of Information Services (OIS).

4.3.2 Employees must make requests for remote access to their supervisors, who must initiate requests to OIS on their behalf. Directors of staff departments must approve requests for their employees, and department chairs must approve requests for faculty members.

4.3.3 Everyone accessing the VPN must authenticate against Active Directory, using their official Technology Account credentials. VPN accounts are automatically disabled when users' Active Directory accounts are disabled upon termination of employment.

4.3.4 Users are removed when directors or department chairs make a request for removal, or when technology staff are made aware of employment terminations.

4.3.5 Authorized users shall protect their login and password, even from family members.

4.3.6 While using an Elmhurst College-owned computer to remotely connect to Elmhurst College's network, authorized users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control.

4.3.7 All hosts that are connected to Elmhurst College internal networks via remote access technologies must use the most up-to-date anti-virus software; this includes personal computers.

## 5. Policy Compliance

5.1 Compliance Measurement

The Office of Information Services (OIS) will verify and promote compliance to this policy through various methods, including but not limited to, reports, internal and external audits, and feedback to individuals and campus departments.

5.2 Exceptions

Any exception to the policy must be approved by the Chief Information Officer in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to network access revocation and personal disciplinary action, up to and including termination of employment.

## 6 Related Standards, Policies and Processes

- *Acceptable Use Policy*
- *Password Policy*