Remote Access Policy

City of Chicopee IT Department for Remote Access

1. Overview

Remote access to the City of Chicopee's (sometimes referred to as "The City" or "City") network is essential to maintain our City's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than the City's network. While these remote networks are beyond the control of the City of Chicopee's IT Department, we must mitigate these external risks the best of our ability.

2. Purpose

The purpose of this policy is to define rules and requirements for connecting to the City of Chicopee's network from any outside network using Chicopee IT issued equipment. These rules and requirements are designed to minimize the potential exposure to the City from damages which may result from unauthorized use of City resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical City internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all City of Chicopee employees with a City-owned computer or workstation used to connect to the City network. This policy applies to remote access connections used to do work on behalf of the City of Chicopee, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to City networks.

4. Policy

It is the responsibility of the City of Chicopee employees with remote access privileges to the City's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the City of Chicopee. Access to sites normally restricted by the City will remain restricted while using remote access connections.

General access to the Internet for recreational use through the City of Chicopee network is strictly limited to City employees (hereafter referred to as "Authorized Users"). When utilizing remote access, Authorized Users are bound by the City of Chicopee *Acceptable Use Policy* and must be followed for as long as the remote access connection is active. Performance of illegal activities through the City network by any user (Authorized or otherwise) is prohibited. Accessing adult-content, gambling, and other non-work related websites and activity is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use City networks to access the Internet for outside business interests.

For additional information regarding City's remote access connection options, including how to obtain a remote access and for troubleshooting, contact the Chicopee IT Helpdesk by submitting a ticket to Helpdesk@chicopeema.gov.

4.1 Requirements
4.1.1   Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs) and strong pass-phrases.

4.1.2   Authorized Users shall not share their login or password, even with family or friends.

4.1.3   While using a City-owned computer to remotely connect to City'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 or under the complete control of an Authorized User or Third Party.

4.1.4   All computers that are connected to City internal networks via remote access technologies must be keep up to date with the latest VPN software, anti-virus, and operating system. If the City computer is not up to date, submit a ticket to Helpdesk@chicopeema.gov.

4.1.5   City VPN software is not authorized to be installed on any personally owned IT device.

5. Policy Compliance

5.1 Compliance Measurement

The Chicopee IT Department will verify compliance to this policy through various methods, including but not limited to, periodic traffic monitoring and reports, internal and external audits, access information and data collection, and inspection, and will provide feedback to the CIO and appropriate Department Head. Chicopee IT reserves the right to terminate active connections or accounts that are deemed to be a violation of this or any associated policy; without notice to the Authorized User.

5.2 Exceptions

Any exception to the policy must be approved by Chief Information Officer (CIO) of the Chicopee IT Department.

5.3 Non-Compliance

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

6   Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of City's network:

- *Acceptable Use Policy*

Remote Access Policy

City of Chicopee IT Department for Remote Access

By signing below, you agree that you have read, understand, and will abide by the City of Chicopee IT *Remote Access Policy*. You acknowledge that while connected to the City's network, you are bound by the City's *Acceptable Use Policy*, which you have read, and will abide by. Please note that this policy and associated policies may be updated without notice to users.

_____   _____
City Employee   Department

_____   _____
City Employee Signature   Date