1. Overview

Remote access to our corporate networks is essential to maintain our team'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 our corporate networks. While these remote networks are beyond the control of the City of Imperial's 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 the City of Imperial's networks which include but are not limited to Enterprise, Wastewater, and Water treatment networks from any host. These rules and requirements are designed to minimize the potential exposure to the City of Imperial from damages which may result from unauthorized use of the City of Imperial resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical City of Imperial internal systems, and fines or other financial liabilities incurred as a result of those losses.

3. Scope

This policy applies to all City of Imperial employees, contractors, vendors, and agents with a City of Imperial-owned or personally-owned computer or workstation used to connect to the City of Imperial networks. This policy applies to remote access connections used to do work on behalf of the City of Imperial, 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 of Imperial networks.

4. Policy

It is the responsibility of the City of Imperial employees, contractors, vendors, and agents with remote access privileges to the City of Imperial's corporate networks to ensure that their remote access connection is given the same consideration as the user's on-site connection to the City of Imperial.

Access to the City of Imperial networks is strictly limited to the City of Imperial employees, contractors, vendors, and agents (hereafter referred to as "Authorized Users"). When accessing the City of Imperial networks from a personal computer, Authorized Users are responsible for preventing access to any City of Imperial computer resources or data by non-Authorized Users. Performance of illegal activities through the City of Imperial networks by any user (Authorized User or otherwise) 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 of Imperial networks to access the Internet for outside business interests.

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

4.1.3 While using a City-owned computer to remotely connect to the City of Imperial's corporate networks, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct City of Imperial business must be approved in advance by the Department of Information Technology (DoIT) and the appropriate business unit manager.

4.1.5 All hosts that are connected to the City of Imperial's internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.

4.1.6 Authorized users should only remotely connect to the City of Imperial's corporate networks during business hours and with an operator request unless special authorization is granted by the DoIT.

4.1.7 All remote access tools or systems that allow communication to the City of Imperial's resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.

4.1.8 Only DoIT approved and configured remote access tools may be used. Connection to the City of Imperial networks will be limited to 7 days, and if more time is needed, it will have to be approved by the DoIT.

4.1.9 VPN users will be automatically disconnected from the City of Imperial's networks after fifteen minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes must not be used to keep the connection open.

4.1.10 By using VPN technology with personal equipment, users must understand that their machines are an extension of the City of Imperial's networks, and as such are subject to the same rules and regulations that apply to the City of Imperial-owned equipment, i.e. their machines must be configured to comply with the City of Imperial's security policies.

5. Policy Compliance

5.1 Compliance Measurement

The DoIT will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

5.2 Exceptions

Any exception to the policy must be approved by the DoIT in advance.

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.

ACKNOWLEDGMENT

If you have additional questions about this policy, please contact Human Resources and/or DoIT before signing the following agreement.

I have read the City of Imperial's Cybersecurity Incident Response Plan and agree to abide by it. I understand that violation of any of the above policies may result in discipline, up to and including termination.

User Name (Printed)	User Signature	Date